APN OLYM2008 使用说明书

OlymIBC Enables e-security

发布日期：2007-12-25

目　录



关于本手册

目的

本手册提供 APN OLYM2008 系列产品的硬件使用安装和调试配置操作说明，并随购买的产品一并附给用户。

版本

版本号：5.0.1 T07-12-25-G2

适用设备版本： APN OLYM 2008 STAR 系列、MOON 系列及 SUN 系列 Release 5.0

如何使用

本手册主要分为硬件安装、系统配置、问答等几大部分。第三章提供了智能向导使用说明，有助于使用者在完成硬件安装后快速了解设备基本配置过程，接着通过第四章内容可以了解到详细的设备配置说明，欲了解 Console 配置方法、工作站设置、VDN 服务管理以及常见问题回答等，请参考第五章以后内容。

本书中采用的特殊标志（文中不再特殊说明）如下：

内容	含义	描述
注意	强调	表示重点提示，对于某些用户易误解的内容作出加重提示说明
加粗斜体	自定义	表示需要用户输入具体要求的正确内容
	警告	表示需要特别注意，设备和数据安全性使用和操作的加强提示
	诀窍	调试配置技巧，可能会帮助管理员节约一定的操作时间
	总结	内容小结，可以帮助管理者快速理解上述过程的重点或步骤

适用对象

本手册适用于购买我公司 APN OLYM2008 系列产品的用户。要求使用者必须具备一定的网络知识和 TCP/IP 基础知识，并且熟悉电子设备的使用和保护。

名词解释

VPN

VPN（Virtual Private Network）即虚拟专网，是利用 Internet 公共网资源、隧道技术、加解密技术及身份认证技术实现企业分支机构互联、soho 办公以及移动接入。

VDN

VDN 又称为 VDN 体系，是我公司独立开发的 VPN 管理和配置技术。不但解决了全动态 IP VPN 网络组建问题，还可以对设备进行管理和服务。

按照 VDN 服务平台的集中管理功能，各终端设备必须到 VDN 服务平台上进行身份认证，并且在认证通过后才能取得相应的跟同一个虚拟域（公司）的其他终端设备进行互连的权限。VDN 通过对进行认证的各节点设备信息的收集、整理和分发，大大简化了终端设备的配置，用户不需要深入学习和掌握 IPSec 协议及相关技术，就能组建起稳定可靠的 IP VPN 网络。

VDN 服务可由奥联科技或运营商提供的 VDN 服务平台实现。也可由带有 VDN 服务模块的 APN OLYM2008 设备提供。

自动隧道

自动隧道是指使用 VDN 服务来建立的 VPN 通讯隧道，该隧道建立过程是将标准 IPSec 配置过程通过 VDN 服务来自动实现。自动隧道建立要求必须具备 VDN 服务下发的许可证信息，该信息由：组域名（Vdomain）、节点名（Vhost）、许可证号（License）三组数据组成，缺一不可，同一组域下的节点设备之间才可以建立自动隧道。

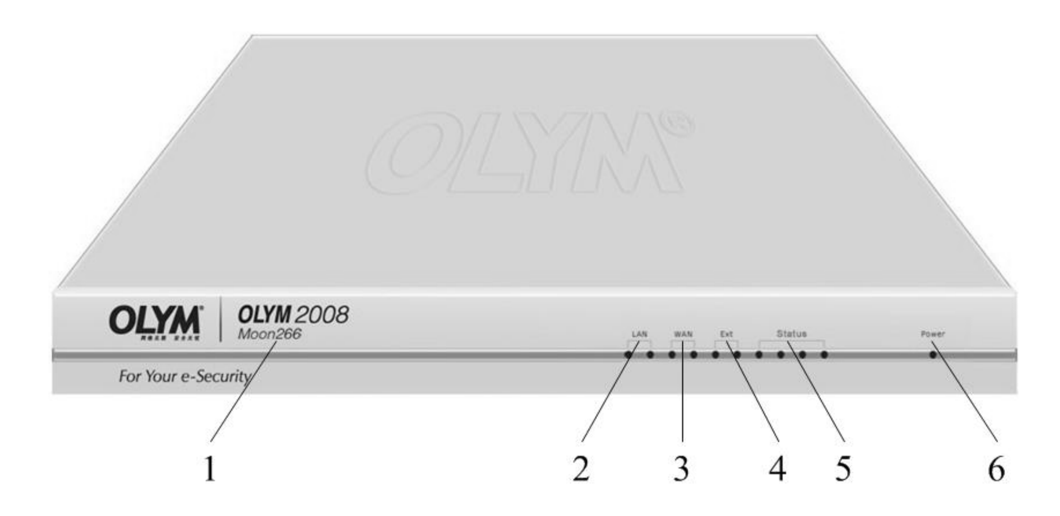
第一章　产品说明

本章主要对 APN OLYM2008 系列产品及其外观布局进行简介

产品概览

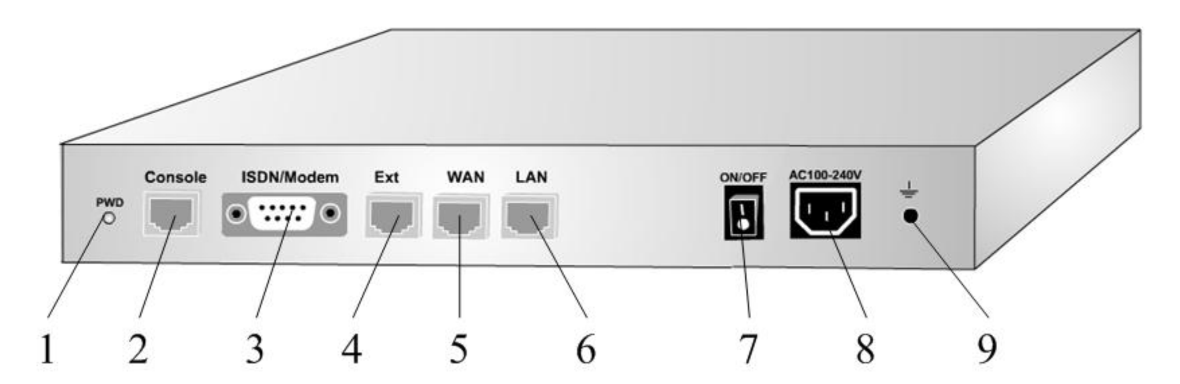
APN OLYM2008 系列产品是基于 IPsec 协议 VPN 安全网关产品，具备 VPN、代理上网、防火墙、网络行为管理等多种功能的智能化网关。为用户提供了全方位网络安全互联解决方案。目前 APN OLYM2008 系列产品已经通过公安部计算机信息系统安全产品质量监督检验中心检验，并且获得了 VPN 和防火墙安全专用产品销售许可证书。

面板视图



1	设备系列及型号标识	**2**	局域网连接 LAN 指示灯	**3**	外网连接 WAN 指示灯
4	扩展口连接 EXT 指示灯	**5**	系统状态 Status 指示灯	**6**	电源 Power 指示灯

背板视图



1 密码恢复 PWD 按键	**2** RJ-45 串口	**3** 电话拨号 Modem/ISDN 接口
4 网络扩展接口 EXT	**5** 外网连接接口 WAN	**6** 局域网连接接口 LAN
7 电源开关 ON/OFF	**8** 电源线接口	**9** 机箱防静电接地

注：APN OLYM2008 STAR 系列设备支持 Boot 重启按键，具体敬请参考实物。

应用拓扑

以深圳、北京、香港为例组建常见应用的 IP VPN 网络，使用 APN OLYM2008 设备的网络应用拓扑如下示：

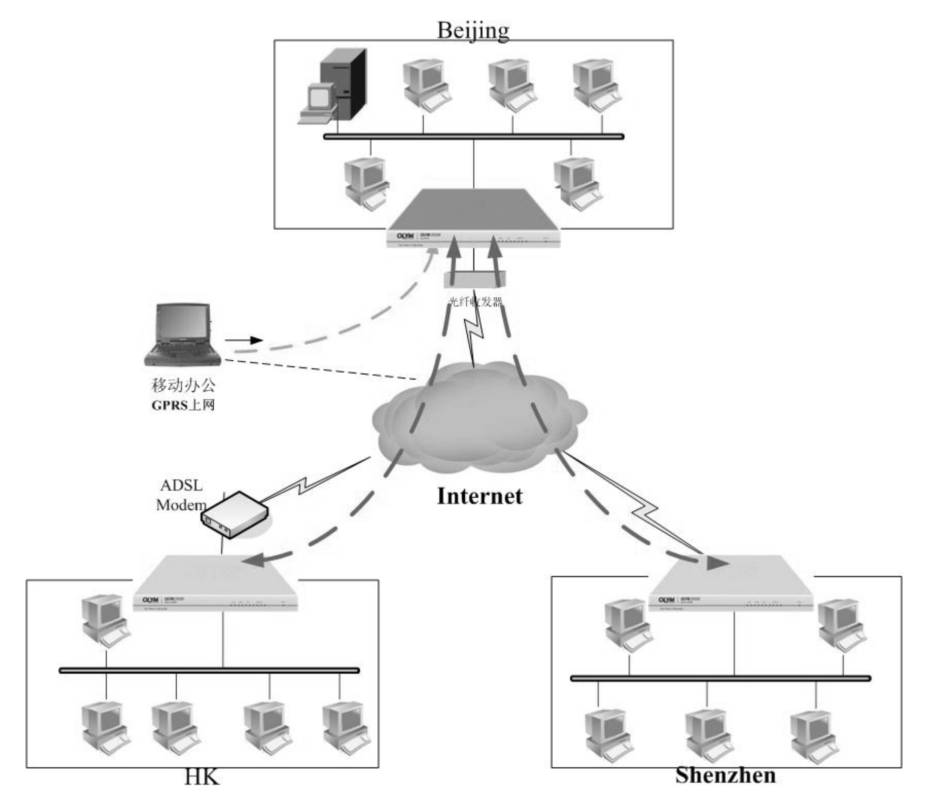


图 1-3：应用拓扑

第二章　硬件安装

本章主要介绍设备硬件安装过程中环境的要求，设备正确使用，配置要求及接口使用说明等。

环境要求

系统正常使用环境要求如下：

- 输入电压：110V~230V
- 功率：STAR 系列最大约 5W、MOON 系列最大约 40W，SUN 系列最大约 100W
- 使用环境温度：0~35 ℃
- 使用环境湿度：5~95%

为保证系统能长期稳定的运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的通风和室温。

安全警告

⚠ APN OLYM2008 系列设备不被允许在酸性、碱性、强磁场等恶劣环境下使用，如因此环境下使用而导致的设备物理损坏将不在本系列产品质保服务之列。

⚠ APN OLYM2008 系列设备属于甲类资讯产品，若需在居住的环境中使用，要求采取适当措施，否则可能会造成无线电干扰。

网管计算机

网管计算机又叫配置电脑，用于调试和管理 APN OLYM2008 设备，在配置设备之前请确认已经符合以下要求：

- **系统要求：**安装超级终端软件的 windows 系列系统均可。
- **硬件要求：**具备 9 针串口（RS-232 标准接口）及网络接口卡（网卡）。

接线

设备接口接线说明图如下：

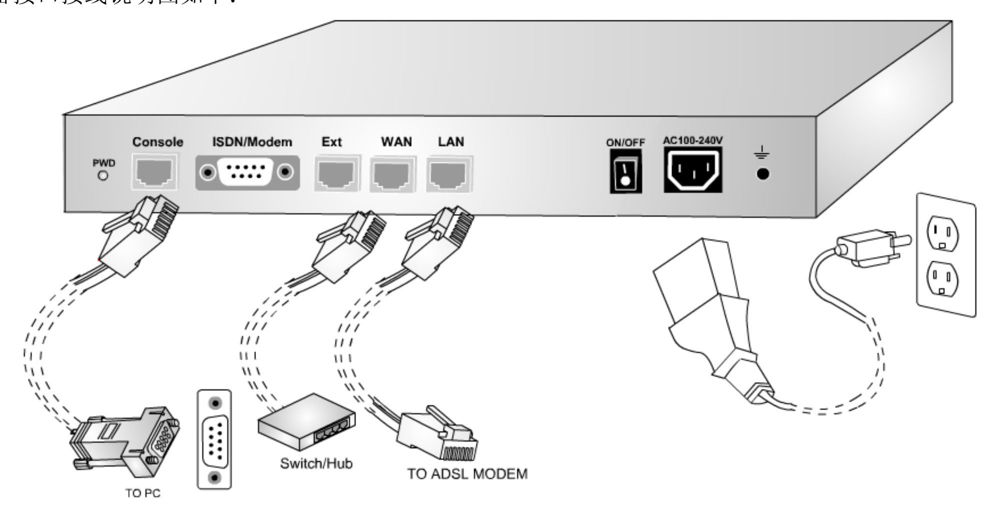


图 2-1：接线示意图

Console 口接线

用于 Console 方式配置设备，使用随机标配的 Console 通讯电缆，将 Console 电缆一端直接与设备 背面板 RJ-45 接口类型的 Console 接口连接，另一端与配置电脑的串口（COM 口）连接。

LAN 口接线

APN OLYM2008 系列产品采用标准 RJ-45 以太网类型接口，通过双绞 （EIA568A 或 568B 线序）网线与本地局域网的网络设备连接，如交换机（Swith），集线器（Hub）等。

WAN 口接线

APN OLYM2008 系列产品支持多种广域联网方式。

- 对于 ADSL 上网方式，用双绞线将 ADSL 猫（Modem）和设备背板标注的 WAN 口连接起来。
- 对于 DDN、Cable Modem、宽带上网的，用双绞线与设备背板标注的 WAN 口连接。
- 对于拨号、ISDN 等方式上网，需要把拨号或 ISDN 的 Modem 连接与设备背板标注的 WAN 口或标 ISDN/MODEM 的接口连接。

EXT 口连接

APN OLYM2008 MOON 系列、SUN 系列或以上系列产品支持硬件扩展口（EXT）应用配置，其接口类型为 RJ-45 标准接口，通过双绞网线与其他网络设备连接。该接口可定义为 LAN/WAN/DMZ。

接通电源

设备使用时，必须保证交流 100V 到 240V 电源。在接通电源开机之前，请保证电源有良好的接地。

第三章　智能向导

本章说明如何利用智能向导进行快速配置及调试设备

使用向导

智能向导可以帮助使用者快速调试设备，点击快捷菜单栏的智能向导图标“ ”，如下图示：

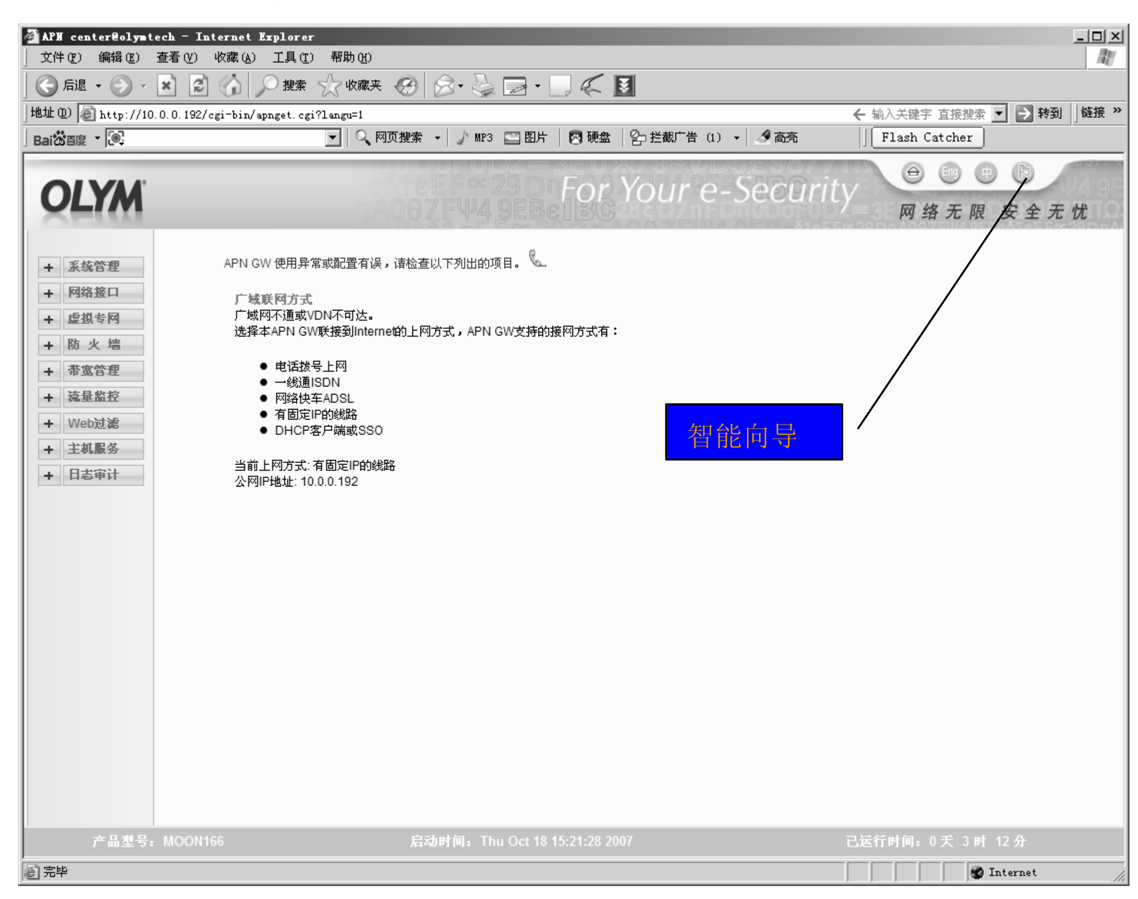


图 3-1：智能向导

参考"智能向导"提示，以"局域网 IP"→ "广域联网方式"→"许可证号"的顺序完成设备的基本配置步骤，即完成后设备即可上网并和其他节点设备连通。

当配置异常时，系统会以红色字体报告，此时可以通过智能向导查询原因或者点击求助电话寻求帮助。

联系奥联

按照智能向导也无法使问题得到解决时，请点击"智能向导"页面的电话图标获得奥联技术支持电话。同时按照向导提示：打开 telnet 和外网访问许可，记录当前设备的 IP 地址。在接通电话后请告知维护人员，方便其快速的进行远程协助维护。

另外可以考虑重启动或者重建隧道动作来快速进行故障排除。

- ☑ **重启动**：热启动设备
- ☑ **重建隧道**：用于当无法访问对端网络或者查看不到隧道信息时快速重建 VPN 隧道。


诀窍：

调试设置一个新的设备，可以直接点击智能向导快速完成基本参数的设置。

第四章　WEB 方式配置

本章介绍使用 Web 浏览器（推荐使用 Microsoft IE5.0 以上版本 ）配置管理设备的操作方法。

系统登陆

连接

首次连接并准备配置 APN OLYM2008 设备时，请参考以下接线连接方式进行连线。

1. 单机环境下设备接线参考图：

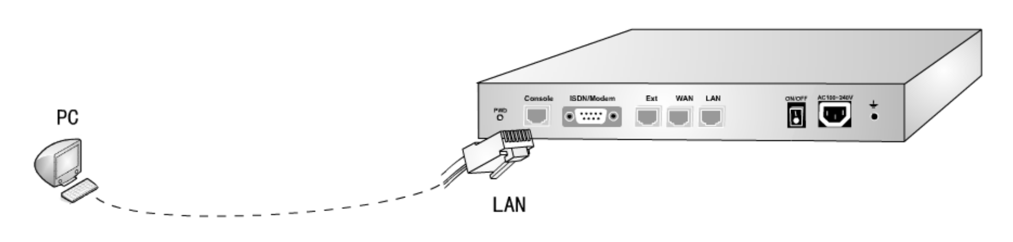


图 4-1：与单机连线图

2. 交换机环境下设备接线参考图：

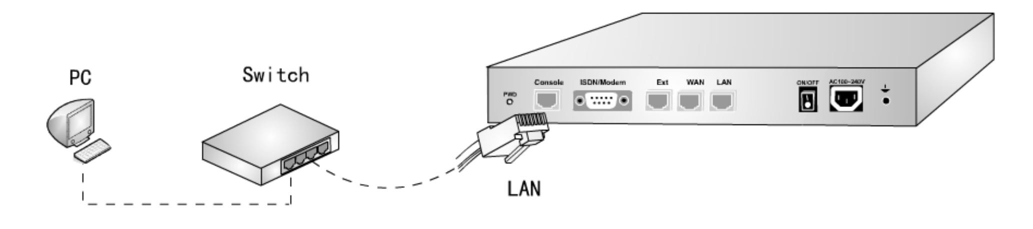


图 4-2：与交换机连线图

登陆

APN OLYM2008 系列设备缺省配置说明：

- 接口缺省 IP：
  - ☑ **LAN IP：*192.168.32.200/24***

- 缺省登陆帐号
  - ☑ 用户名：***root***
  - ☑ 密码：***gw1admin***

无论将应用于简单还是复杂的网络连接环境下，首次配置设备，请按照下面方法进行网络设置连接并登陆设备进行配置管理

(一)配置电脑 IP 设置

设置配置电脑和 APN 设备缺省 LAN IP 为同一个网段，例如您可以设置：

- IP 地址：***192.168.32.100***
- 子网掩码：***255.255.255.0***
- 默认网关：***192.168.32.200***

(二)连接登陆设备

配置电脑设置完成后，打开IE浏览器并输入：http://192.168.32.200/，如下图示：

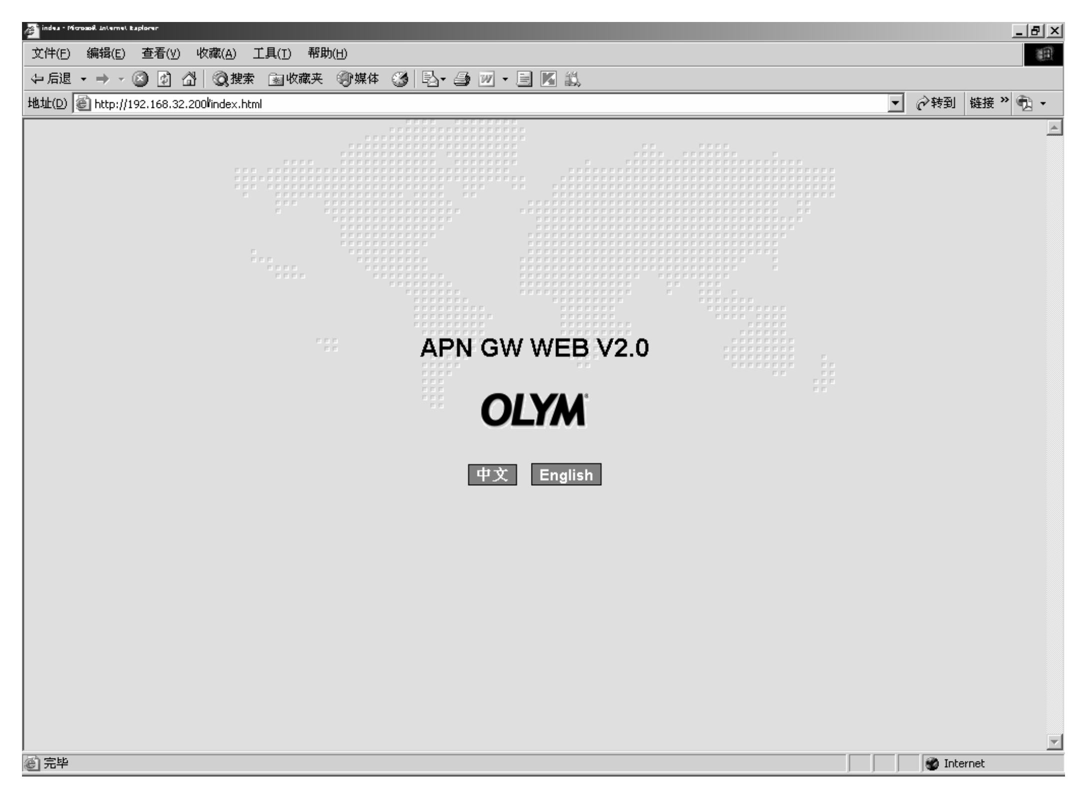


图 4-3： 设备初始登录界面

选择“中文“或“英文”，登陆用户验证通过后就可进入主配置界面了，下面将以中文配置界面进行配置管理介绍。

用户验证

设备对任何连接到其系统的管理员要求身份验证，验证通过才能登陆进行配置、维护及管理，如下图

示，按提示要求输入：

用户名：***root***

密码：***gw1admin***（以*显示）



图 4-4：登陆帐号验证窗口

界面布局

系统界面分为菜单栏、主配置界面、状态栏及快捷操作栏，如下图示：

图 4-5：管理界面

(一)菜单栏❶：

- **系统管理：** 系统基本管理及运行状态查看。如：系统用户管理、时间设置、密码设置、系统资源、系统信息查看、备份与恢复，维护等等；
- **网络接口：** 设备接口信息、广域网连接方式、扩展口应用、静态路由等设置管理；
- **虚拟专网：** VPN 隧道配置管理，如：自动隧道管理、虚拟专网特性参数设置、手工隧道设置、移动用户接入服务端设置、子网共享设置、隧道信息查看等。
- **防火墙：** 广域许可、防火墙访问控制管理、地址转换等应用设置管理。
- **带宽管理：** 局域网带宽占用优化及分配管理设置。
- **流量监控：** 网络流量信息、内网会话连接情况，上网 URL 记录等信息的统计查看。
- **Web 过滤：** 限制用户上网行为及访问内容的设置，如：主机黑白名单管理，url 屏蔽规则设置、关键字屏蔽等；
- **主机服务：**常用网络服务。如：远程登陆服务（Telnet）、Web 服务、SNMP Agent、多播转发、DHCP、DNS、动态域名服务（DDNS）、双机热备、MAC 地址绑定等。
- 日志审计： 系统日志查看或日志存储配置。

(二)主配置界面❷：

主配置界面提供功能说明及配置项目索引服务，用户通过界面相关文字指导可以对系统的功能进行简单了解，并链接至相关项目配置清单。

(三)快捷操作栏❸：

：点击该按钮可以快速的返回系统初始登陆界面进行语言切换选择。

Eng：点击此按钮可以直接切换到英文管理界面

中：点击此按钮可以直接切换至简体中文管理界面

：智能向导按钮，用于指导用户进行快速配置及调试设备

(四)状态栏：

产品型号❹：显示当前设备所属的产品系列及其型号
启动时间❺：显示启动使用的时间

系统管理

系统信息

系统信息包括：系统版本、防火墙版本、客户端版本、系统发布日期、VPN 认证状态隧道信息、当前防火墙策略数、接口配置信息及状态报告等信息。根据系统信息提示，管理员能够快速了解到设备当前配置及运行状况，对于异常情况作出及时处理。



图 4-6：系统信息

(一) 系统状态

系统状态	
产品型号	STAR88
版本号	5.0
APN防火墙版本号	3.0
APNSEC版本号	1.4
WINAPN版本号	3.0
建立号	20071206

图 4-7：系统状态

- ☑ 产品型号：是指设备硬件系列及其型号，如 STAR88 表示当前使用设备为 STAR 系列，型号为 88。
- ☑ 防火墙版本号：系统当前防火墙版本为 3.0
- ☑ **APSEC** 版本号：IPsec 客户端版本号
- ☑ **WIN** 版本号：移动客户端版本信息，客户必须按照此处的信息安装客户端才能够正常接入网络
- ☑ 建立号：系统版本正式发布的日期，如 20071206 表示系统当前运行版本是在 2007 年 12 月 6 日正式发布。

(二) 认证状态

认证状态	
当前APN組域	olymtech
节点名	404
状态	已成功接入

图 4-8：认证状态

- ☑ **当前组域：** 是指用户在 VDN 服务器上申请的虚拟域名，一般是根据用户公司名称确定的，比如 olymtech。
- ☑ **节点名：** 指在虚拟域里定义的设备名称，比如 404、test020、host001。
- ☑ **状态：** 节点接入 VDN 服务器进行认证的状态，比如成功接入，等待应答等，不同的状态反映了到 VDN 平台认证是否成功。

(三) 防火墙策略数

防火墙策略数	
防火墙策略数	136

图 4-9：防火墙策略数

- ☑ **防火墙策略数：**显示了当前系统所有防火墙的策略总数目。

(四) 隧道数

隧道	
最大隧道数	128

图 4-10：隧道数

- ☑ **最大隧道数：**显示了设备所支持的最大ＶＰＮ隧道数目，不同系列不同型号设备支持的数目不同。

(五) 移动客户端

移动客户端	
支持最大用户数	5
在线用户数	1

图 4-11：移动客户端数

- ☑ **支持最大用户数：**缺省情况下显示了设备系统当前标配所支持的最大同时接入的客户端数目，根据设备的型号，用户可以订制所需的数目。
- ☑ **在线用户数：**显示了当前已经接入的客户端数目。

(六) 公网 **IP**

公网IP	
当前上网方式	网络快车ADSL
IP 地址	121.15.34.4
当前链路状态	已连接

图 4-12：公网 IP 信息

- ☑ **当前上网方式：**显示了设备外联网络的连接方式。如光纤固定 IP 线路、ADSL 线路或其他。
- ☑ **ＩＰ地址：**当前外网接口的 IP 地址，当是固定线路就是配置 IP 地址，当是 ADSL 就是自动获得的 IP 地址，如果无显示 IP 地址，即可判断外网连接是异常的。
- ☑ **当前链路状态：**是指设备外网连接状态，正常情况为认证成功。

(七) 内网 IP

内网IP	
IP地址	192.168.32.200
MAC地址	00:02:b3:02:02:02
子网掩码	255.255.255.0

图 4-13：内网 IP 信息

- ☑ **ＩＰ地址：**设备内网接口地址，一般为局域网网关地址。
- ☑ **ＭＡＣ地址：**设备内网接口卡物理地址
- ☑ **子网掩码：**用于判断 IP 标识网络中主机所属的网络及其主机地址。

系统资源

系统资源用于显示当前设备各项资源的消耗情况。包含 CPU 的负载，存储器使用空间，网络的并发连接数目等情况。

在使用设备过程中，通过该功能可以监控系统的资源情况，帮助管理员判断设备是否处于正常的运行状况。



图 4-14：系统资源查看界面

(一) 基本信息

显示当前设备型号及版本（如 STAR88）、组域号、节点名、版本发行日期、WINAPN 版本、防火墙版本等。

APN STAR88	
VDOMAIN	olymtech
VHOST	404
Build No	20071206
WINAPN	3.0
Firewall	3.0

图 4-15：系统基本信息

(二) 系统时间（system time）

如下图示，通过显示系统运行开启时间和运行天数间接显示了系统无故障运行的状态。

System time	
启动时间	Thu Dec 6 19:42:35 2007
已运行时间	0天 18时 35分

图 4-16：系统运行时间

(三) CPU 使用

显示设备历史和当前 CPU 使用率情况。根据 CPU 使用情况间接的可以了解内网状态，一般可能是病毒引起 CPU 处理大量数据造成的资源耗损。

CPU使用	
CPU之前使用率	Total: 50647085
397672(0.79%)	50249413(99.21%)
当前 CPU使用率	Total: 103
3(2.91%)	100(97.09%)

图 4-17：CPU 使用情况

(四) 存储容量使用：

存储系统由内存、虚拟磁盘及磁盘存储器构成。存储容量使用显示当前系统占用存储空间的情况，给用户进行配置管理设备提供资源占用参考。

存储容量使用	
内存 ＋虚拟磁盘(kB)	Total: 61376
47792(77.87%)	13584(22.13%)
虚拟磁盘(kB)	Total: 29745
19843(66.71%)	9902(33.29%)
磁盘(kB)	Total: 6400
664(10.38%)	5736(89.62%)

图 4-18：系统存储情况

- ☑ **"内存＋虚拟磁盘（KB）"**栏表示出总内存容量、已经使用的容量和空闲容量；已经使用的容量包含虚拟盘占用的空间和系统进程运行占用的内存空间。
- ☑ **"虚拟磁盘（KB）"**栏表示出从内存上划出多少来做虚拟盘，已经使用了多少虚拟盘空间。虚拟盘是用于装载系统。
- ☑ **"磁盘"**栏表示出设备储存器（DOC 或者 flash）中用于保存配置信息的空间、已经使用的空间和剩余空间。

(五) 网络并发访问数

网络并发是上网时点对点连接的会话数，系统网络并发访问数显示通过设备当前会话连接数。该数值变越大，预示着内网异常很可能出现。

网络并发访问数	
会话	Total: 16384
108(0.66%)	16276(99.34%)

图 4-19：网络并发数

密码更改

鉴于系统安全的考虑，建议在使用缺省帐号及密码登陆系统后，尽快更改设备缺省帐号的密码。

访问管理--密码更改	
原来的密码:	
新密码:	
新密码确认:	
	提交 重置

图 4-20：密码更改配置界面

密码修改要求说明：

1）. 新密码和旧密码十分相似，将被拒绝。例如原来密码为 gw1admin 改为 gw2admin；

2）. 新密码过于简单，将被拒绝.例如 1111111。

对于字典里的常用单词、或者全是大写或全是小写的以及没有包含数字或特殊字符的字符串是不能用来做密码的。建议用下面的规则设置有效的密码：

1）. 密码至少要有 8 个字符，最好包含一个以上的数字或特殊字符。

2）. 密码不能太简单，所谓的简单就是很容易猜出来，例如：自己的名字，电话号码、生日、职业或者其它个人信息等。

3）. 密码必须是有有效期的，要求在一段时间之后必须更换密码。

4）. 在日志里面若发现有人试图多次猜测密码，强烈建议立即修改。

时间设置

时间设置可使设备时间和任何能够管理系统的计算机进行同步，系统时间是否准确会直接影响移动客户端的正常接入以及防火墙时间计划策略的生效，所以，建议首次配置设备时，最好检查系统时间是否已经为当前工作时间。

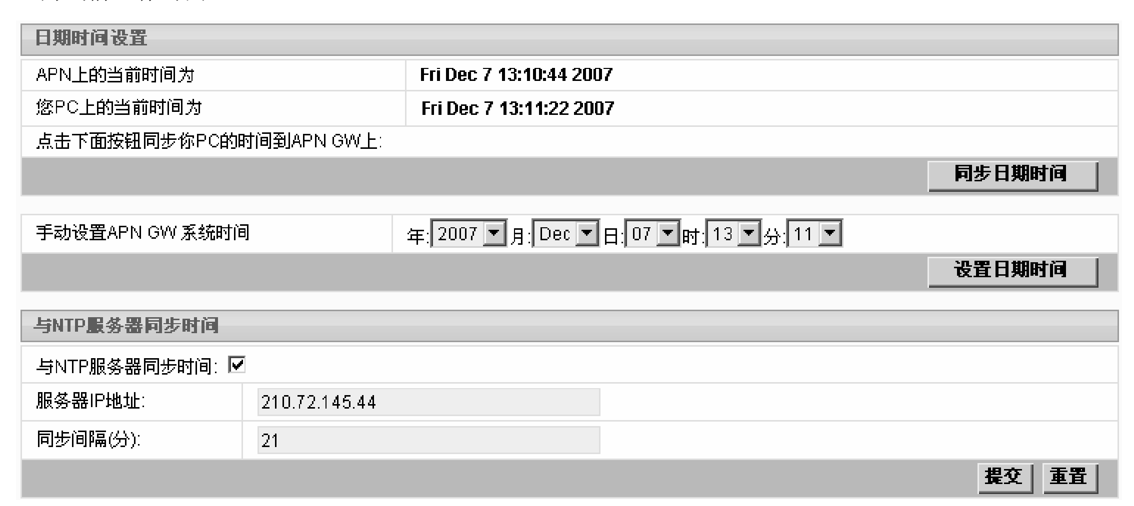


图 4-21：时间设置界面

可以手工设置或者与电脑时间同步。

另外，通过开启"与 NTP 服务器同步时间"，并指定正确的 NTP 服务器 IP 及同步间隔，设备会在设置的时间间隔后进行时间同步。

系统维护

系统维护管理包括对配置文件的备份和恢复、出厂设置及服务状态管理等。

恢复配置

如需将设备已经备份的配置文件恢复到新设备或者正在使用的设备上，使用恢复配置功能，如下图示：

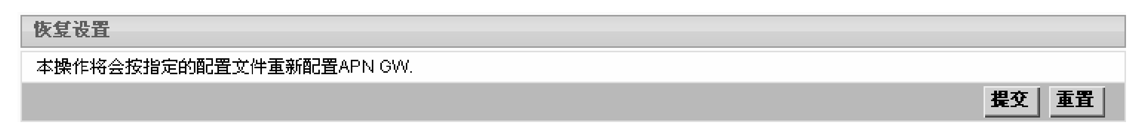
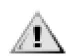


图 4-22：恢复系统配置界面

按“提交”按钮后，确认保存路径，原来备份的配置将会恢复到系统中，恢复完成后系统提示“重启设备”。

 警告：不同型号设备之间配置文件不能互相导入。

备份配置

每次完成设备配置后，建议使用备份配置功能将全部的配置文件备份到本地计算机，作为用于日后恢复所用。

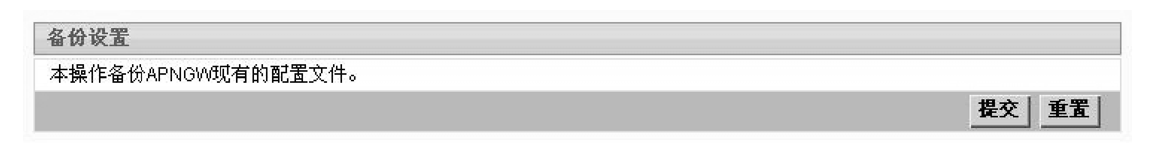


图 4-23：备份配置界面

按“提交”按钮后设备会自动收集系统配置信息，并将其作为一个文件（.bin）保存至网管计算机.建议将配置文件保存于系统安全的目录下。

出厂设置

出厂设置是设备出厂时的缺省配置状态，该功能用于将系统文件配置清除并恢复至缺省配置。

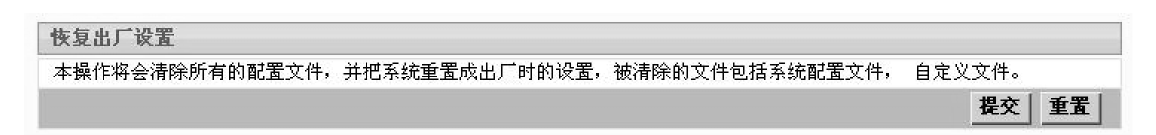


图 4-24：恢复缺省配置

建议进行出厂恢复设置之前，做好系统备份或重要信息（许可证信息）备份，以免因此给工作带来不必要的麻烦。

服务状态

服务状态显示了当前系统已经开启和未开始的服务状态，如下图示，已勾选为已开启服务。

服务状态显示
远程登录: ☑
WEB服务: ☐
SNMP: ☐
多播转发: ☐
域名服务: ☑
动态IP分配: ☐
动态域名服务: ☐
双机热备份: ☐

图 4-25：服务状态

系统工具

ping 和路由跟踪 tracert 工具常用于 windows 系统判断其系统到某个目的地址的链路是否连通以及 IP 路由的情况。APN OLYM2008 系列产品也支持 ping 和 tracert。

(一) Ping

Ping是用来进行网络通讯链路检测的主要程序， 通过ping可以进行检测设备到网络中的任何主机的连通性。如下图所示，输入要检测的目标主机的地址，点击"提交"即可开始检测。例如：检测设备是否和220.181.6.6这台网络主机连通。

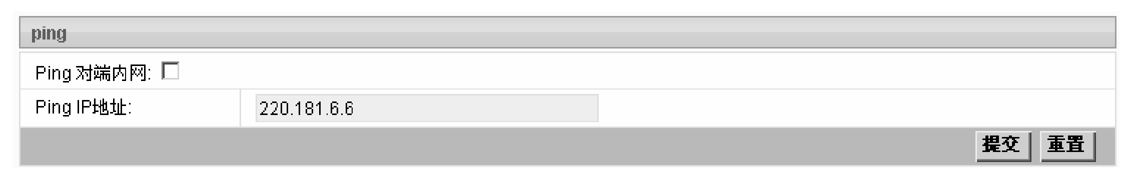


图 4-26：ping 检测

点击"提交"稍等片刻可以看到 ping 结果（有关 ping 的结果请参阅资料获悉）。

(二) Tracert

tracert 是网络路由跟踪程序，可以让我们看到数据包从网络里一台主机到网络中另一台主机的所经过的路由。在 设备里可以直接使用该命令跟踪一个数据包从设备到达另一个设备或者网络其他主机的路由情况。

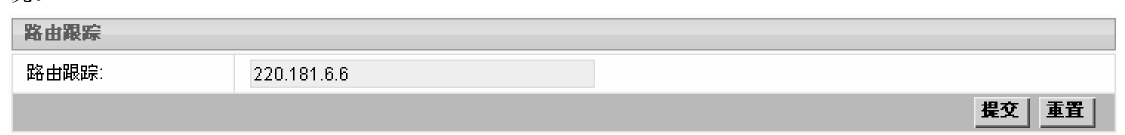


图 4-27：路由跟踪

设置跟踪检测目标 IP 点击"提交"，系统开始路由跟踪探测并将跟踪结果显示出以供管理员管理分析。

网络接口

网络接口配置包含局域网 IP、广域联网、静态路由及 MAC 地址修改等。

局域网 IP

局域网 IP 用于配置设备 LAN 口 IP，使其能够正常连接到本地局域网，并与内部主机进行通讯。



图 4-28：局域网 IP 设置界面

按照局域网 IP 地址设置提示设置

☑ **IP 地址：**设置 LAN 口的 IP 地址，一般作为局域网的默认网关

☑ **子网掩码：**按照网络规划设置正确的掩码地址，如 A 类、B 类、C 类

☑ **工作模式：** 设备当前工作模式支持自动协商（Auto）、10/100M 全双工、10/100M 半双工，需要根据接入设备接口的工作模式选择，缺省自动协商模式

☑ **重启 APN GW:** 勾选该选项并“提交”后设备会重新启动。

注意：

❶ 设置新的内网 IP，或者重新设置接口速率和模式后，必须重启设备后才能生效；

❷ 重启设备后，必须修改计算机的网段跟设备的 LAN IP 网段一致，才能继续进行配置；

❸ 内网口的网段不应该跟其他网口、移动用户及需要互通的其他地方设备使用的网段一样。

当需要在内网口绑定多个网段或者相同网段的多个 IP 时，可以添加“接口别名”， 删除一个接口别名配置，点击对应操作栏的删除按钮“”即可删除。如下图示：



接口别名

IP地址	子网掩码	操作
192.168.133.1	255.255.255.0	
192.168.135.1	255.255.255.0	
192.168.136.1	255.255.255.0	提交 重置

图 4-29：局域网接口别名

广域联网

广域联网用于设置设备外连网方式，比如 ADSL，固定 IP 线路、小区宽带、串接路由或防火墙等等方式，根据实际连接的线路进行正确选择及设置即可。另外广域联网配置还提供了广域连接调试如关闭或者重联操作。如下图示：

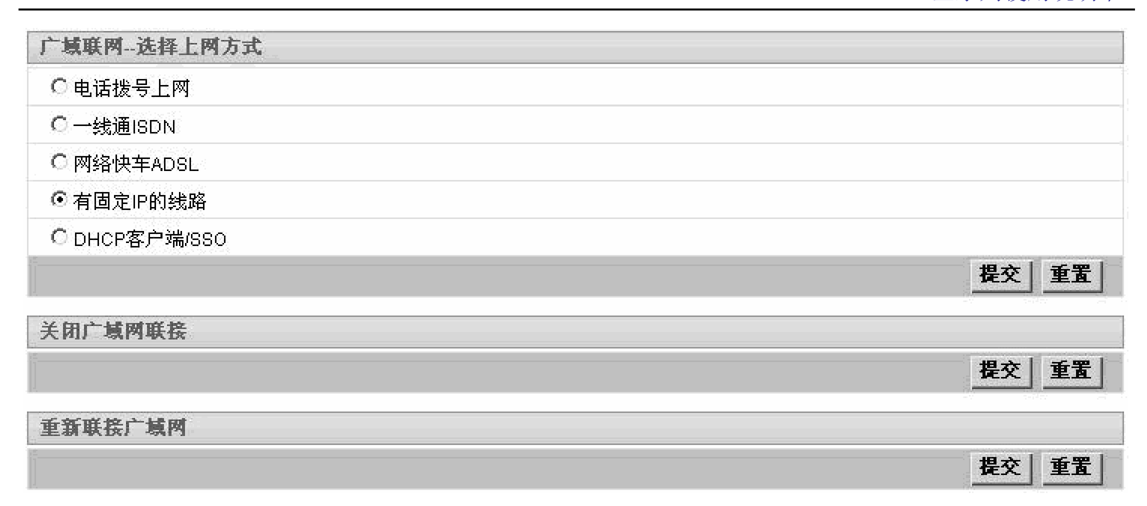


图 4-30：广域联网方式

(一) 上网方式选择

设备支持多种上网方式，在多种可选的上网方式中确定选择一种正确的方式后，按"提交"按钮后，进入相关配置窗口，按照提示输入必要的参数。

1. 有固定 IP 的线路

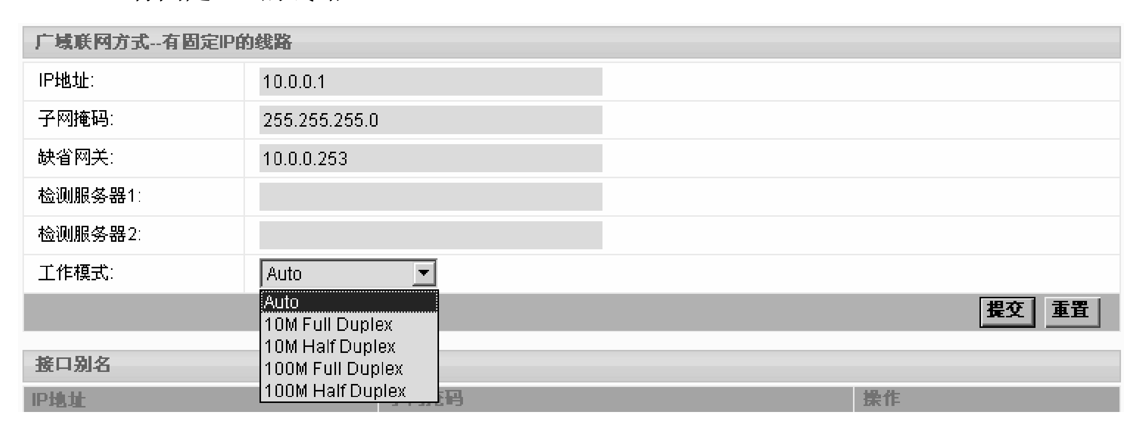


图 4-31：固定 IP 上网方式配置界面

- ☑ **IP 地址：** 由 ISP 分配的 IP 地址，需要正确填写
- ☑ **子网掩码：** ISP 分配 IP 所提供的掩码地址，必须正确填写
- ☑ **缺省网关：** ISP 提供的线路缺省网关地址，必须正确填写
- ☑ **检测服务器：** 用于对于线路连接状态检测，一般填写公网可用的服务器 IP 地址。

另外，为了保证外联线路的正常， 设备支持线路检测服务，有必要可以设置检测服务器 1 或 2（可以同时设置），以保证联网正常。

当固定线路如光纤线路，有绑定多个 IP 时，当设置完主 IP 后，可以根据应用需要，以添加 "接口别名" 的方式在外网口绑定多个 IP。如下图示：点击"添加"给 WAN 口添加多个 IP，需要删除时，点击操作栏上的删除按钮" "即可。



接口别名		
IP地址	子网掩码	操作
10.0.0.140	255.255.255.0	
10.0.0.112	255.255.255.0	
		添加

图 4-32：广域网接口别名

绑定多个 IP 后，可以在防火墙的目的地址转换设置中将 IP 或者指定端口映射到内部的服务器上。

注意：

❶ 重新设置接口速率和模式后，必须重启设备后才能生效。

❷ 当外网口需要设置私有 IP 地址连接外网时（如安装在小区、大楼共享环境或者已有防火墙后面时），建立自动隧道需要进入“虚拟专网”→“启用内网穿透”。

2. 网络快车 ADSL

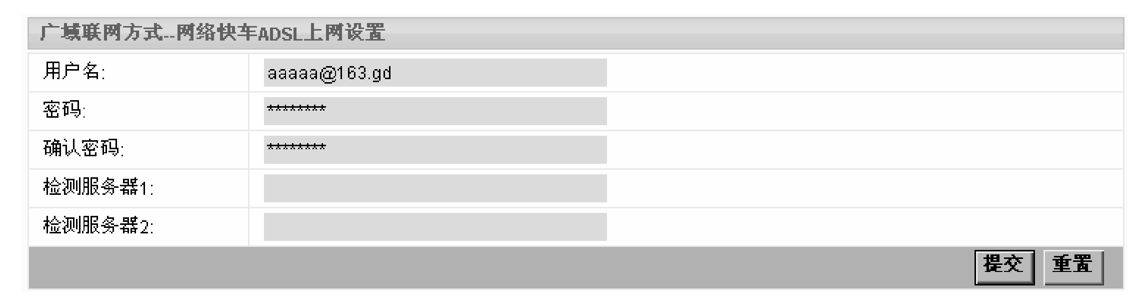
动态 IP 上网方式 ADSL，支持标准的 PPPOE 拨号方式，当采用该方式上网时，可按照如下配置过程进行拨号设置：

进入“**广域联网方式--网络快车 ADSL 上网设置”**配置界面，配置以下信息：

☑ **用户名**：ADSL帐号，例如aaaaa@163.gd。

☑ **密码及确认密码**：ADSL 帐号密码。

☑ **检测服务器 1、2**：可用公网 IP 地址，用于检测 ADSL 线路可靠性。



广域联网方式--网络快车ADSL上网设置	
用户名:	aaaaa@163.gd
密码:	********
确认密码:	********
检测服务器1:	
检测服务器2:	
	提交 重置

图 4-33：ADSL 设置

判断设备是否成功拨号并获得动态 IP，点击“网络接口”回到“基本网络设备界面”，在下图椭圆圈处将会显示当前外网口的连接状态及其成功获得 IP 地址的情况





图 4-34：基本网络设置

(二) 关闭广域联网

暂时停止广域联网使用“关闭广域联网”，在如下图点击“提交”即可使设备与外网联接断开。

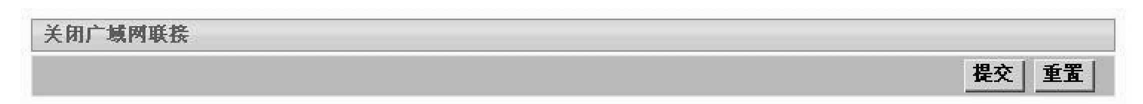


图 4-35：关闭广域联网

(三) 重联广域联网

关闭广域联网或者网络因异常断开了与外网的联接时，使用重联广域网功能即可使设备主动尝试联接，在如下图“提交”即可。



图 4-36：重联广域网

静态路由

OLYM2008 全系列产品支持静态路由设置，用于多个内部网段通过静态路由来实现互通。

例如：添加一条从本地到本地另一网段 10.0.1.0 网络的静态路由，如下图示，如果要删除路由信息，点击“ ”即可删除。

路由设置					
目的网络	子网掩码	网关	跳数	接口	编辑
10.0.1.0	255.255.255.0	192.168.138.1	2	内网口	
1.1.1.0	255.255.255.0	10.0.0.138	2	外网口	
	255.255.255.0			内网口	提交 重置

图 4-37：静态路由设置

注意：

❶ 对于只有外部接口为固定 IP 地址设置时，才能外部接口的静态路由。比如，外网口是 ADSL 的 PPPOE 拨号上网方式时，不能为此接口设置静态路由。

❷ 当 EXT 口设置作为外网扩展接口时，第一链路和第二链路由于检测失败而中断后，对应于此接口的静态路由会丢失，链路恢复后，静态路由不会自动恢复。

MAC 地址修改

MAC 地址是网络接口卡（网卡）的物理地址，由厂商在出厂时写入的，具有唯一和固定性，不可随意修改。由于实际使用中经常受到使用限制而需要修改，所以 OLYM2008 系列产品支持 WAN 接口卡和 EXT 接口 MAC 地址修改功能。如下图示：

在对应接口 MAC 修改处直接输入新的 MAC 地址，点击“提交“即可修改成功。

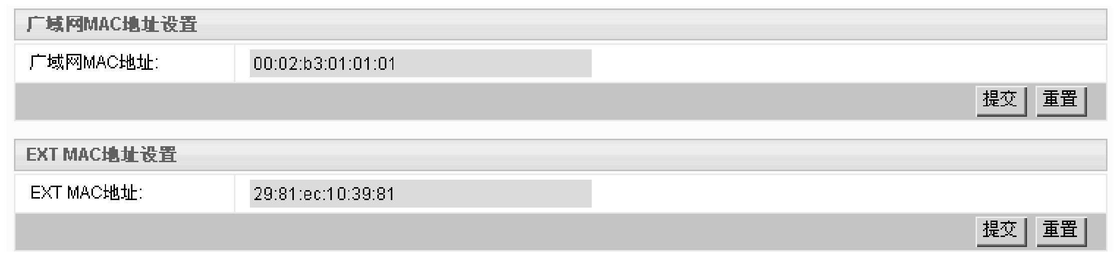


图 4-38：MAC 修改

注意： MAC 地址修改并保存后需要重启设备后才能生效。

DMZ IP

DMZ 为非军事防御区，作为对外的服务器区，该区域对外和对内都是允许被访问的，但禁止该区向内部主机发出的任何服务请求。

例如：某企业内网网段为 192.168.133.0/24，为了保证局域网不受外网的恶意攻击，同时又要对外提供 web 服务以扩大企业的宣传力度。为了解决这一问题，我们可以在内部设置一个新的网段 192.168.135.0/24 作为 DMZ 服务网段，DMZ 网关 192.168.135.1/24，那么具体设置如下：

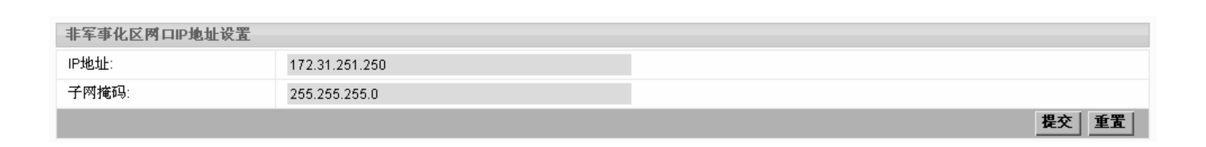


图 4-39：DMZ 区 IP 配置界面

注意：

❶ DMZ 的网段不应该跟其他网口、移动用户及需要互通的其他节点设备使用同一网段。

❷ 对外的服务器的网关必须指向该 DMZ IP 才能保证服务正常。

EXT 接口的扩展

EXT 口缺省作为 DMZ 接口，另外根据需求可以扩展为内网接口或者外网接口来使用。如下图示：

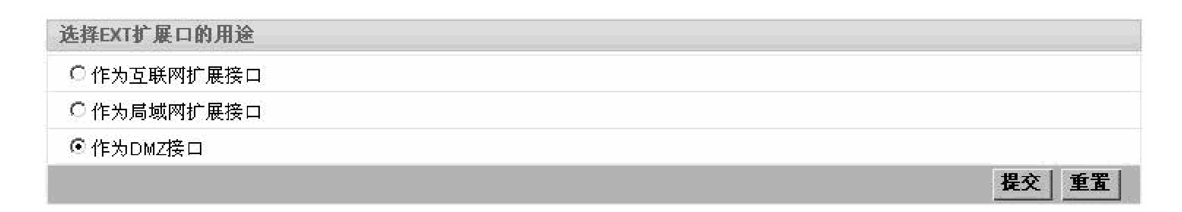


图 4-40：EXT 接口作用扩展界面

注意：部分型号设备不具备 EXT 接口。

EXT 口作为内网扩展接口

进入"扩展网口设置"，选择"作为局域网扩展接口"，然后点击"提交"按钮。刷新页面后，进入"扩展局域网口 IP"， 设置分配给扩展接口的 IP 地址和掩码。内部网络可以有单独的物理网络通过此接口连接互联网、通过隧道访问对方网络，以及访问局域网口的内部网络。如下图所示：

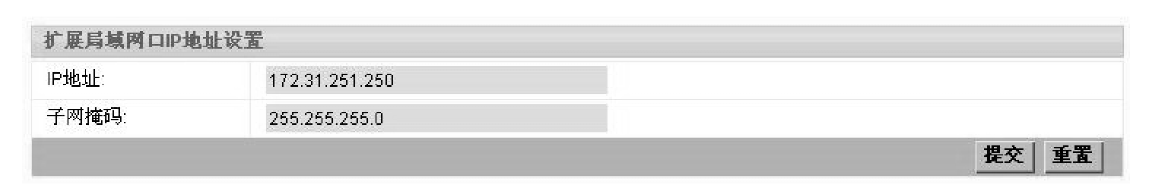


图 4-41：EXT 扩展为局域网口配置界面

注意： 内网口的网段不应该跟其他网口、移动用户及需要互通的其他节点设备使用的网段一样。

EXT 口作为外网扩展接口

进入"扩展网口设置"，选择"作为互联网扩展接口"，然后点击"提交"按钮。出现如下图示扩展链路模式选项

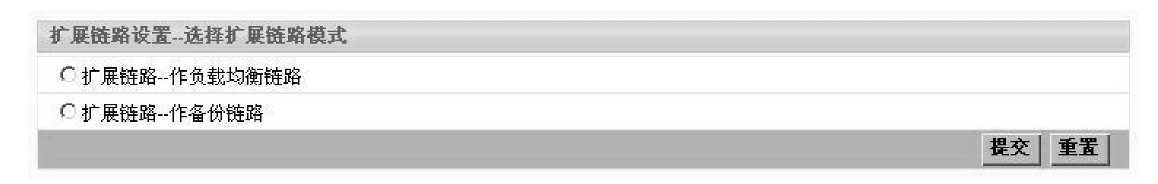


图 4-42：EXT 口扩展负载均衡链路

1) 作为负载均衡链路

选择"扩展链路-作负载均衡链路"，按"提交"按钮后，出现：



图 4-43：负载均衡链路属性配置界面

☑ **"第一链路恢复后，隧道自动切换回第一链路"选项：** 当两线路正常时，设备通过第一条线路建立自动隧道；当第一链路中断后，设备通过第二条线路建立自动隧道。 在第一条线路恢复后，如果需要跟对端设备建立的隧道自动切换回第一线路，需要选择此项；

☑ **多链路上网带宽比重：** 设定线路上网带宽占用比例。如需两线路实现均衡，设定为 1:1；如需专门使用第一条线路跟对端建立隧道承载业务数据，第二条线路用来上网，设定为 1:100（可为任意）;

☑ **链路设置：** 设定线路检测目标。线路通断是通过 ping 设定的目标 IP 检测的。对设定的两个 IP，每隔 10 秒 ping 一个包，如果连续 6 次没有 ping 通，系统会认为此线路中断。当其中一条线路中断后，隧道、上网流量会切换到另一条正常线路上。

重新点击"网络接口"，进入"第二链路设置"，如下图，根据备份链路情况选择和设置相应上网方式。

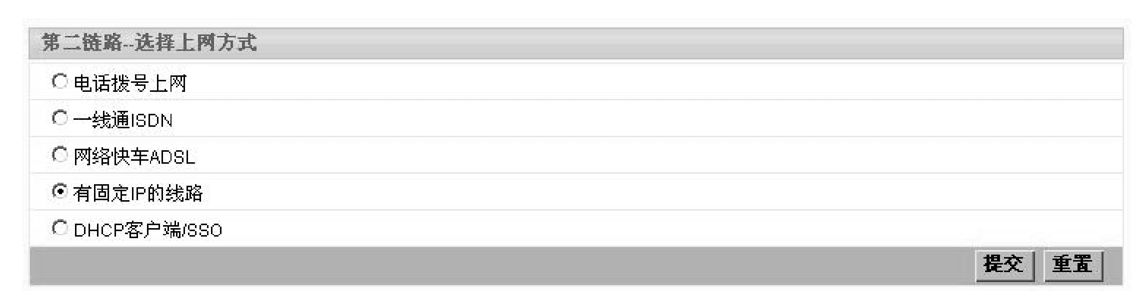


图 4-44：第二链路方式选择

2) 作为备份链路

选择"扩展链路-作备份链路"，按"提交"按钮后，如下图示：

线路检测服务器地址(互联网备份链路---备份属性)		
第一链路:	61.145.112.53	: 211.152.9.59
备份链路:	211.152.9.59	: 61.145.112.53
		提交 重置

图 4-45：备份属性配置

☑ **链路设置：** 敬请参考负载均衡链路设置。

重新点击"网络接口"，进入"备份链路设置"，如下图示，根据备份链路情况选择和设置相应上网方式。

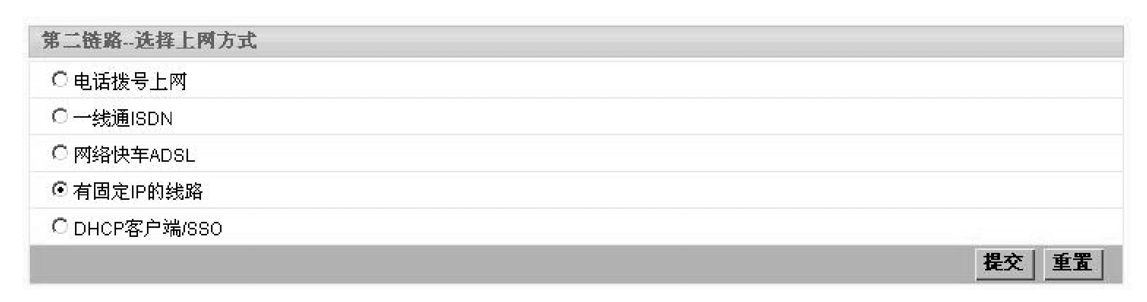

第二链路--选择上网方式
○ 电话拨号上网
○ 一线通ISDN
○ 网络快车ADSL
⦿ 有固定IP的线路
○ DHCP客户端/SSO
提交 重置

图 4-46：第二备份链路选择

注意：

以上检测目标IP设置应该为公网可靠的主机或服务器IP。比如：www.163.com网站的IP。当发现异常检测失败时，需及时修改检测目标。

虚拟专网

OLYM2008 系列设备 VPN 设置分为自动隧道和手工隧道两种方式。

自动隧道模式用于进行许可证配置管理，提供全动态网络服务；手工隧道则是完全符合 IPsec 协议配置标准，用于和其他 IPsec VPN 进行 VPN 隧道建立设置。

许可证号

许可证号是使用自动隧道服务必需具备的数据包，在配置前敬请确认已经具备正确数据，或者联系相关管理人员获取该正确信息。如下图示，许可证号信息包括：

APN组域,结点名,许可证设置	
只使用手工隧道: ☐	
APN组域(VDOMAIN):	wenquan
节点名(VHOST):	test020
许可证号:	x9Y9l4Bs8e9fSmHPnDY997Fv
共享密码:	public
现在激活: ☐	
	提交 重置

图 4-47：许可证信息配置

- ☑ **“只使用手工隧道”选项：** 用于设备在非自动隧道的情况下使用的选项，勾选提交后，自动隧道功能将失效。
- ☑ **组域、节点名、许可证号：** 使用自动隧道的认证信息，请联系相关管理员获得正确信息 。
- ☑ **共享密码：** 由总部网管统一指定的字符串， 有效长度为 1-30 个数字或者字母组合，各互连的设备设置必须相同。
- ☑ **“现在激活”选项：** 用于使以上设置立刻生效的选项，选择此项后再按“提交”即可

注意：

❶ 同一个许可证不能在多台设备上同时使用

❷ 建立自动隧道的设备必须具有相同的共享密钥

专网特性

专网特性是指根据不同网路应用限制和需要对 VPN 网络进行特殊参数配置的管理服务。

(一) 隧道类型

设备支持三种 VPN 隧道协议：IPsec 、IPIP、GRE。“隧道类型”选项缺省为 IPsec。当所有节点都具有公网 IP 上网方式，并且通信不要求加密时，就可以选择 IPIP 或 GRE 类型。IPIP 和 GRE 类型可以带来更高的传输性能。

● IPsec 隧道类型

设备支持标准 IPsec VPN 协议，该协议提供了数据传输可靠性验证，不可抵赖性认证，具体配置说明如下：



图 4-48：IPsec 隧道具体参数配置

1. 数据传输属性设置：

- ☑ **“数据加密算法”选项：** 缺省为 AES/128。可以选择 NULL（不加密数据）、AES/128、3DES/168、

SCB2、Serpent/128、Twofish/128、Cast/128 其中一种。

- ☑ **“传输认证算法”选项：** 缺省为 MD5-96。可以选择 MD5-96、SHA1-96、SHA2-256、SHA2-512 其中一种。
- ☑ **“传输压缩传送”选项：** 例如用户可以根据需要对加密算法、传输认证算法等数据传输进行调整设置；如果大多数的地方的设备是通过 modem 拨号等低速率线路上网，同时选择此项。

注意：必须保证建立隧道的所有设备参数配置一致。建议使用缺省配置。

2. 支持私有 IP 接入公网

该功能是指 NATT 功能配置，即不具备公网 IP 而联入互连网的属性设置：

- ☑ **“启用内网穿透”选项：**当网络中有设备处于内网，即外网口与路由器等其它网络设备连接时，就必须启用该选项。
- ☑ **“内网穿透组号”：**当网络中有两个或以上的节点设备处于同一个 NAT 设备下，并使用自动隧道通信时，则必须在这些设备上设置相同穿透组号，穿透组号有效范围为 1-65534。

注意：

❶ 当选择”启用内网穿透”后，并未指定组号则为缺省 65535，此时表示不会建立自动隧道。

❷ 在 NAT 下的两个相同组号的节点设备，只要外网口 IP 能互通，相互之间就能建立自动隧道。

❸ 启用内网穿透的上网设备，都能跟具有公网 IP 的节点设备建立自动隧道。

3. 扩大本端子网范围

使用自动隧道时候，缺省情况下 VDN 会将设备局域网段作为本端子网和对端建立隧道。但有时需要扩大本端的掩码范围，则可使用此功能。

例如：本地 APN 网段是 192.168.0.0/24，但是通过本地交换机还可以访问 192.168.1.0/24、192.168.2.0/24 的网段。远程 APN 的网段是 172.16.0.0/24。缺省情况下，自动隧道只是建立了从 192.168.0.0/24 与 172.16.0.0/24 的隧道，当远程互联网络需要通过自动隧道同时访问该三个网段时，则需要设置：

- ☑ **“扩大子网”选项：**启用”本端子网掩码”扩大功能设置。
- ☑ **“本端地址”：**是设备内网口 IP 地址，用于自动隧道监测目标 IP。只有选择了”扩大子网”后，此设置才有意义，不建议修改。
- ☑ **“本端子网掩码”：**是指按照 IP 地址掩码划分网络原则将已有的网络地址范围扩大，从而将内网的所有网段聚合为一个大的网段，即最大限度把所有的网段归纳为一个网段网络。

根据上述例子，则可设置本端子网掩码为 255.255.252.0。也可以设置为更大范围的子网掩码，比如：255.255.0.0。

如果需要隧道对端网络在上网时，必须先通过本端设备，然后再出互联网，可将本端子网掩码设置为 0.0.0.0。

注意：扩大后的网段不能和对端设备下的网段冲突。比如：远端为 192.168.0.1/255.255.0.0，本端掩码扩大后为 192.168.101.1/255.255.0.0。并且可能需要设置 APN 访问本地其它网段的静态路由。

4. **“启用交叉巡检”选项：**用于隧道经常出现中断且不能自动恢复情况，选择此项可以使设备进行自动隧道检测和隧道连通恢复

5. **“启用突发巡检”选项：**用于外网线路经常出现中断且不能自动恢复的情况，选择此项设备会自动进行线路检测和断线重连

- **IPIP 隧道类型**

IPIP 协议是一种对不加密数据传输的隧道协议。设置参数如下图示，具体设置项不再赘述，敬请参考 IPsec 隧道类型相关项说明。

遂道类型: IPIP 编辑

扩大本端子网范围	
扩大子网: ☐	
本端地址:	192.168.138.1
本端子网掩码:	255.255.255.0
遂道自检与自动恢复	
启用交叉巡检: ☑	
启用突发巡检: ☑	
现在激活: ☐	
	提交 重置

图 4-49：IPIP 隧道配置

- **GRE 隧道类型**

GRE 协议可以译为通用路由协议，也是一种非加密数据传输的隧道协议。设置参数如下图示，具体设置项不再赘述，敬请参考 IPsec 隧道类型相关项说明。



图 4-50：GRE 隧道配置

注意： 两端必须为公网 IP，才能建立可通信的 GRE 隧道。

定点检查汇报

定点检查汇报用于当 VPN 链路作为专用线路的备份时，与 VDN 配合可实现线路的自动备份，自动恢复，并能进行故障情况报警和记录。如下图示，设置项包括：

☑ **“启用定点检查汇报”选项：**启动定点检查汇报功能，只有在指定待检测目标 IP 底之后才生效。

☑ **“待检测目标 IP 地址”：**需要检查的设备外网 IP 地址。

☑ **“通过环路返回”选项：**可选项设置，启用后会环路返回线路异常报告。

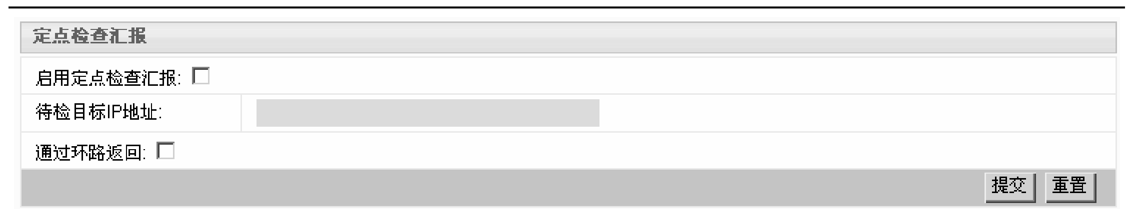


图 4-51：定点检查汇报

隧道信息

当设备之间自动隧道建立成功后，在”隧道信息”里，就可以看到有关本地节点设备和其他节点设备间的隧道信息：对端网段，公网 IP，隧道状态（Up/Hold）等。

在线结点列表(此页信息每隔120秒刷新一次)				
本地结点名（本地局域地址段）		对端结点名（对端网络地址，对端公网IP）		隧道检测
Up	@test.test001	@test.test002		
0	192.168.165.0/255.255.255.0	192.168.32.0/255.255.255.0	%any	提交
对端在线结点合计: 1				

图 4-52：隧道信息

注意： ❶ 本处显示的隧道信息不包含手工隧道的信息。

❷ 隧道状态分为“Up”和“Hold”，“Up”表示当前自动隧道连通可用，“Hold”则表示隧道已断开

手工隧道配置

手工隧道配置用于标准 IPsec 协议协议配置，分为隧道基本特性、IKE 第一阶段及 IKE 第二阶段配置。该方式主要用于跟远端其他厂家的 IPsec VPN 设备建立隧道或者不使用 VDN 服务的情况。

(一). 隧道配置

手工隧道配置可以分为三步骤：”隧道基本特性配置”→“IKE 第一阶段配置”→“IKE 第二阶段配置”。

1. 隧道基本特性配置

隧道基本特性包括建立隧道的当前上网线路性质及 IP 地址，及其将在建立隧道过程中处于的主动还是被动状态模式，具体参数如如下图示：

隧道基本特性

本地网络模式

有固定IP的线路 192.168.131.25

对端网络模式

有固定IP的线路

自检设置

指定供隧道检测的存活主机的IP地址

启动状态

◉ 无操作

○ 客户端

○ 服务器端

图 4-53：隧道基本特性

☑ **本地网络模式**：分固定 IP 和非固定 IP。

- **固定 IP 的线路**： 当本地的上网模式为公网固定 IP 或者公网 IP 映射私网 IP 的情况下，此时对应的 IP 地址必填。
- **非固定 IP**： 指动态 IP 地址方式（如 PPPOE，DHCP），NAT 方式等

☑ **远端网络模式**：分固定 IP 和非固定 IP。

- **固定 IP 的线路**： 当本地的上网模式为公网固定 IP 或者公网 IP 映射私网 IP 的情况下，此时对应的 IP 地址必填。
- **非固定 IP**： 指动态 IP 地址方式（如 PPPOE，DHCP），NAT 方式等

☑ **自检设置**：隧道自动愈合功能设置，启用该功能必须提供一个供检测的 IP 地址，该 IP 地址必须为隧道建立成功后允许通过隧道 ping 的一台存活主机，一般为对端设备内网口地址，或者对端网络内的一个主要服务器或者主机 IP 地址。

☑ **启动状态**：隧道在设备启动后进行连接的模式，分为"无操作"、"客户端"、"服务器端"。

- **无操作**：表示设备在启动后不对这个手工隧道信息做任何处理。激活隧道则需要人工操作。
- **客户端**： 表示设备在启动后会自动的发起尝试跟对端建立隧道。
- **服务器端**： 表示设备在启动后以被动身份等待客户端发起建立隧道请求，才进行当前隧道建立。

注意：本地和远端的网络模式不能同时选择为**非固定 IP**

2. IKE 阶段 1

如下图示，IKE 第一阶段需要配置如下参数：

IKE阶段1	
隧道名称	
第一阶段模式:	
◉ 主模式	
○ 野蛮模式	
认证方法	
◉ 预共享密钥	如果预共享密钥为空，则使用默认值
○ 证书（未支持）	
ISAKMP SA 密钥周期	
1	密钥周期的单位是小时，默认是1小时，最大值是8小时
ID	
本地ID	
对端ID	

图 4-54：IKE 阶段 1

- ☑ **隧道名称**：不同隧道标识名，可以是任意的英文字母加数字的组合。最长不能超过 64 个字符。
- ☑ **第一阶段模式**：IKE 协商第一阶段的模式，分主模式和野蛮模式两种。主模式更安全，野蛮模式协商速度更快，一般建议使用主模式。
- ☑ **认证方法**：IKE 协商的认证方法，分为预共享密钥（PSK）和证书认证，标准版本只支持 PSK，PSK 密钥最长不超过 128 位。
- ☑ **ISAKMP SA 密钥周期**：密钥周期以小时为单位，默认值为 1 小时，最大值为 8 小时。
- ☑ **ID**： ID 有三种格式，所有建立隧道的设备都必须设置相同格式的 ID，并且建立隧道的两端需要互相对应。比如 A 和 B 建立隧道，在 A 上配置**本地 ID** 为 a@a.com,**对端 ID** 为 b@b.com,那么在 B 上必须配置**本地 ID** 为 b@b.com,**对端 ID** 为 a@a.com。

注意：

❷ 此项在**远端**的网络模式为固定 IP 的情况下为必填项，且两个设备相互建立**多条隧道**的时候只能使用一个 PSK（**注意** PSK 的一致，否则隧道可能无法建立成功）；当远端网络为非固定 IP 的情况下，PSK 使用的是默认的值，欲修改该值，请点击”许可证号”链接，修改共享密钥的值并提交。

❷ 当对端设备在使用 PSK 身份认证必须使用野蛮模式时，本端也必须选择野蛮模式。

❸ ID 的 3 种形式：

1. IP 地址形式，如：222.222.222.222。
2. 域名的形式（Fully Qualified Domain Name）：如：abc.authcyber.com。设备系统会将此域名解析为 IP 地址。不建议使用此种形式，当设备本身的 DNS 设置并不能解析此域名到正确的 IP 地址时，则会出现异常错误。
3. user@FQDN 或@FQDN 的形式。系统不会尝试将@后面的域名解析为 IP 地址。

---

3. IKE 阶段 2



图 4-55：IKE 阶段 2

- ☑ **保护套件**：包括数据加密算法、传输认证算法、是否启用完全向前保护（PFS）选择。数据加密算法和传输认证算法为隧道建立后对所传输的数据的保护算法；PFS 为更强的防重发攻击的一种机制，启用该功能将增加设备的资源损耗，第二阶段协商的时间更长。
- ☑ **链路模式**：分为隧道模式和传输模式两种。一般选用隧道模式，因为设备一般都是作为网关型设备的应用。
- ☑ **两端子网**：支持隧道模式的选项，指定建立隧道的设备的内网网段地址。
- ☑ **数据封装协议**：IPsec 支持 ESP 和 AH 的数据封装，一般选择 ESP 更安全，它提供数据的加密和完整性认证保护。
- ☑ **IPsec SA 密钥周期**：密钥周期以小时为单位，默认值为 8 小时，最大值为 24 小时
- ☑ **压缩**：是否进行数据压缩传送。

注意：

❶ 手工隧道和自动隧道可以并存。

❷ 设备设备跟其他 VPN 产品互连 ，跟 VDN 无关。

❸ 手工隧道不支持全动态 VPN 互连。但如果对端设备支持 DDNS 设置，可以使用 DDNS 设置；

❹ 当两边都没有公网 IP 时（两边都是通过 NAT 方式上网时），作为服务端的一端，在其前的 NAT 设备上必须进行端口映射，将 UDP500 和 UDP4500 端口映射到上才能正常建立隧道；

❺ 两端子网设置，当为点对点的网络模式的时候，建立隧道的两端所填写的子网必须是对应的才能建立隧道；当为点对 any 的网络模式的时候，该点必须在对端子网处填写 0.0.0.0，且子网掩码必须选择为 0.0.0.0

❻ 如果要启用压缩，那么建立隧道的两端必须同时启用压缩才能建立隧道，建议只在网络带宽非常小的情况下使用，启用压缩将增加设备的资源损耗。

(二). 当前隧道状态

当前隧道状态显示了本地和对端 VPN 设备之间隧道的状态及相关信息，如对端子网及公网 IP 地址。当需要对隧道进行操作时，可以通过"隧道管理"来进行隧道断开、监听、激活等操作。



当前隧道状态

状态	名称	本地子网	对端子网	对端公网IP	隧道管理	隧道检测
●	test	192.168.138.0/24	192.168.32.0/24	192.168.135.56	激活 提交	不支持

新增隧道

状态标注: ●表示连接正常 ●表示连接异常或处于监听状态 ●表示未启用

图 4-56：当前隧道状态列表

移动用户

移动客户端用户移动办公用户接入网络服务，其隧道验证支持预共享密码（PSK）认证、文件证书及 IBCKey 文件证书认证方式。用户在任何地方，只要能够上网，都可以安全、轻松配置使用。



图 4-57：移动客户端配置管理

客户端使用详细说明不在此阐述，敬请参考相关《客户端使用说明书》文档，该文档可以从随机光盘或者www.olymtech.net 网站下载。

子网共享

子网共享功能是自动隧道功能的扩展应用，适用于远程网络和本端内网多个网段同时通过设备进行自动隧道访问的应用。

例如： 192.168.1.0/24、10.10.10.2.0/24 是本地网络，现远程网络需要通过隧道访问所有的网段

根据分析发现这两个网段并不能通过尽量长的掩码完全聚合为一个网段，所以需要进行子网共享设

置，子网共享功能设置如下示：

子网共享						
IP地址	子网掩码	网关	APN组域	节点名	许可证号	编辑
192.168.139.1	255.255.255.0	192.168.138.1	olymtech	host01	KQOAFpsoKn2pZexer1L3Xm1B	
192.168.135.1	255.255.255.0	192.168.138.1	girlly	apn	at9nFbljPnTQFy1r	提交 重置

图 4-58：子网共享配置

☑ **IP 地址：** 对端需要访问本端的第二个网段的网络地址，比如：192.168.139.1。此项不为空。

☑ **子网掩码：**对端需要访问本端的第二个网段的子网掩码，比如：255.255.255.0。此项不为空。

☑ **网关：**设备到达此共享网段的下一跳路由器 IP，此项可为空。

☑ **组域、节点名、许可证号：**在 VDN 上为此设备新生成的信息，请联系相关管理员获得。相互之间需要建立隧道的设备，组域号必须相同。

注意：

❶ 通讯的两台设备不能同时启用“子网共巷功能”。

❷ 所有设备和使用子网共享的设备建立自动隧道时，都必须具有公网 IP。

❸ 多个网段和一个网段同时建立隧道时，应该按照先“扩大掩码”、再“子网共享”的原则。

高级参数配置

高级参数配置分为：**缺省模式**和**快速模式**。高级参数配置参数显示了设备比较灵活的连接认证机制，这样可以提高设备的工作的可靠性。缺省模式如下图示：

高级参数设置: 缺省模式 编辑	
基准时间	5 (s)
重发认证包速率	7x5 (s)
重认证速率	300x5 (s)
隧道巡检间隔	60x5 (s)

图 4-59：缺省模式

当需要使用快速模式时，点击高级参数设置“编辑”按钮选择快速模式，如下图示

高级参数设置: 快速模式 编辑	
基准时间	5 (s)
重发认证包速率	1x5 (s)
重认证速率	50x5 (s)
隧道巡检间隔	20x5 (s)

图 4-60：快速模式

VDN 地址设置

当设备组域、节点名和 license 等信息是由厂家以外的 VDN 提供服务，那么必须修改设备缺省指向的 VDN 地址值（cache）。即先将 VDN IP 地址解析为 cache，并配置到每个节点设备。具体配置如下图示：



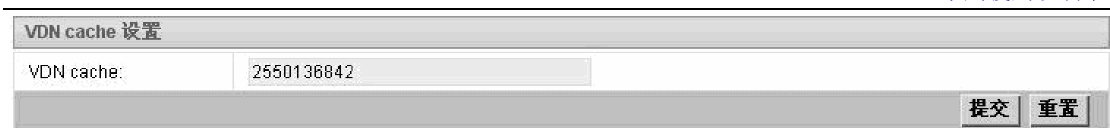


图 4-61：VDN cache 设置

完成 VDN cache 值配置，点击“提交”即可生效，此时需要重新激活“许可证号”或者重启设备，才能连接新 VDN 进行服务认证。

防火墙

设备防火墙是基于状态检测包过滤、应用层协议过滤及对象设置管理技术，其当版本可能会因系统软件的升级而进行而升级，详细信息敬请关注www.olymtech.net网站通知。

广域许可

为了保证设备在线安全，设备防火墙缺省禁止管理者从互联网或者 VPN 隧道对端对其进行配置和管理的同时，还支持用户对系统的自主开放和分配管理主机的功能。

(一) 广域许可管理

广域许可是允许管理者从设备外网对其进行配置和管理。

如下图，在”防火墙”→“广域许可”中，勾中“允许从广域网访问本机”后“提交”即可。

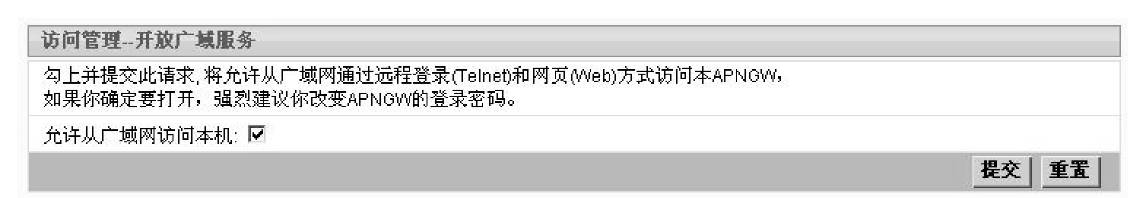


图 4-62：广域许可

这时，互联网中的任意计算机和互联网的计算机都可以通过 Web 和 Telnet 方式连接设备，在拥有管理帐号情况下就可以登录管理设备。

注意：

打开“允许从广域网访问本机”的选项。这样，互联网上任意计算机都可以尝试登陆此设备。因此强烈建议完成设备设置管理后及时关闭该选项。

(二) 可信的管理主机设置

可信的管理主机功能是指设备允许不可信网络里值得信任的主机对其进行管理维护。

例如：允许总部网段 192.168.0.0/24 的网络管理员对设备进行随时维护；61.145.112.53 这个互联网的 IP 是绝对可信任的，维护人员可以通过这个 IP 地址的服务器随时维护本机。如下图所示。

可信的管理主机		
IP 地址	子网掩码	Edit
192.168.138.35	255.255.255.0	
61.145.112.53	255.255.255.0	
192.168.0.0	255.255.255.0	
		添加

图 4-63：可信的管理主机

网络对象管理

防火墙网络对象包括：节点对象、子网对象及节点组对象，具体是指：

☑ **节点对象**：是指网络中的主机

☑ **子网对象**：是指一个网络或者一个网段

☑ **节点组对象**：是指一组主机的集合

注意：防火墙内置对象为内网/[LAN]、外网/[WAN]、APN 网/APNNET、DMZ/[DMZ]、[ANY]

❶内网/[LAN]：是指本地局域网网段，即是指与内网口（LAN）直接连接的网络。

❷外网/[WAN]： 内网、APN 网及 DMZ 以外的网络。

❸APN 网/[PNNET]：指任何 VPN 隧道对端网络。

❹DMZ/[DMZ]：非军事防御）区。

❺ [ANY]： 是指所有网络。

---

1. 节点对象

一个节点对象具有以下属性，属性必须正确设置，否则会导致防火墙规则不生效，具体说明如下：

☑ **节点名称**：用于标识主机的名称，有效字符为英文、数字组合。长度为 1 到 32 个字符，禁止使用防火墙内置关键字作为节点的名称，如 LAN、WAN、APNNET、ANY。

☑ **IP 地址**：主机的 IP 地址

☑ **MAC 地址**：主机的 IP 地址对应得网卡地址，其有效格式必须:XX:XX:XX:XX:XX

☑ **所属网络**：根据实际指定主机的网络位置：内网、外网或者 APN 网络。

例如： 需要定义一些内部局域网的主机对象，例如名为 administrator，IP 为 192.168.138.5、MAC 地址为 00:DB:00:EC:A5:13 的对象、还有 Bob、John，对于 Allice 由于其地址经常不固定，所以可以直接定义 MAC 地址，另外还可以定义外网地址如 Webserver，网络的 ERPserver 等对象。

具体设置如下图示：

节点对象				
节点名称	IP地址	MAC地址	所属网络	编辑
BOb	192.168.138.10		内网	
John	192.168.138.200	00:FF:03:7E:E8:25	内网	
administrator	192.168.138.5	00:DB:00:EC:A5:13	内网	
Allice		00:13:02:72:53:B9	内网	
Webserver	211.152.9.59		外网	
ERPserver	192.168.1.100		APN网	
				添加

图 4-64：节点对象

完成添加后"提交"保存。点击编辑栏" "即可删除对象，对于定义错误或者修改的对象，点击修改按钮" "

可进入修改状态进行修改。

2. 子网对象

一个子网对象具有以下属性没，属性必须正确设置，否则会导致防火墙规则不生效，具体说明如下：

- ☑ **子网名称**：用于标识子网的名称，有效字符为英文、数字及其组合，字符长度 1-32 位。
- ☑ **IP 地址**：子网 IP 网段或者 IP 地址。
- ☑ **子网掩码**：所要定义的子网的正确掩码（根据所定义子网网络地址的长度换算）例如：255.0.0.0/255.255.0.0/255.255.255.0/或者其他正确的掩码。
- ☑ **所属网络**：指定子网的实际位置：内网、外网、APN 网络。

子网对象

子网名称	IP地址	子网掩码	所属网络	编辑
GOwan	192.168.139.0	255.255.255.0	内网	
GOlan	211.135.23.156	255.255.0.0	外网	
APN1	192.168.133.0	255.255.255.0	APN网	
				添加

图 4-65：网络对象

设置完成后“提交”保存，删除子网对象点击编辑栏的“ ”可删除，修改点击“ ”进修改状态进行修改。

3. 节点组

把多个主机划分为一个组，进行访问控制限制，不但可以节省添加相同控制规则的目的，还可以简化访问控制规则设置。


节点对象组

组名称	编辑
tech	
market	
	新建节点对象组

图 4-66：节点对象组

例如： 要定一个一个名称为 Gonet 的节点对象组，其成员包括 zgn、Bob、John（此三个节点事先已经定义好了）。 具体做法步骤如下：

a 新建节点对象组

在如下图示界面右下角，点击“新建节点对象组”


节点对象组

组名称	编辑
tech	
market	
	提交 重置

图 4-67：新建节点对象组

点击“提交”设置成功即可进入该对象组组员添加界面，点击“添加”进入如下图示界面，在节点对象名称下拉框选择需要的对象。

b 添加组成员

第一次新建节点对象组时，系统则直接进入节点成员添加界面，另外可以随时给节点对象添加成员，如下图示，添加时，点击对象组名称对应编辑栏的“ ”进入节点对象成员添加界面，删除一个未被规则引用的对象组则点击“ ”按钮即可删除。

节点对象组	
组名称	编辑
tech	
market	
	新建节点对象组

图 4-68：添加节点对象组成员

点击“添加”进入如下图示界面，在节点对象名称列表直接选择对象名称，提交方才生效。



图 4-69：节点对象添加

删除节点对象成员，点击对象组里成员对应编辑栏“”即可删除

注意：

❶ 删除一个节点对象组，必须确认该对象组没有被防火墙任何规则引用

❷ 删除节点对象组里的成员不会删除该节点对象在防火墙里的定义

服务对象管理

为了使用方便，设备内置了常用的网络服务，可以任意引用于防火墙控制规则，甚至可以删除。

但是在日常应用中，有很多专业软件使用的服务端口，比如 ERP 软件，SQL 数据库服务等等，此时需要自定义服务对象。

1. 添加服务对象

服务对象属性包括：

- ☑ **服务名称：** 用来标识所定义服务，有效字符大小写英文、数字及其组合，长度 1-32 字符。
- ☑ **协议：** TCP 或 UDP。
- ☑ **端口：** 是指实际应用的服务端口如 80（HTTP）、1433(SQL)。
- ☑ **源起始端口：** 设置端口段的起始端口。
- ☑ **源结束端口：** 设置端口段的结束端口。

例如：某个专业 C/S 软件服务器端对外提供服务的协议端口是 UDP3000~UDP4000 范围内的，则按照如下示方法来添加该服务对象，定义服务名称为 APPsoft。

如下图，修改或者删除时，点击器编辑栏对应的操作按钮即可。

服务对象

服务名称	协议	端口	源起始端口	源结束端口	编辑
HTTP	tcp	80			
HTTPS	tcp	443			
FTP	tcp	21			
TELNET	tcp	23			
SMTP	tcp	25			
POP3	tcp	110			
SMTPS	tcp	465			
POP3S(TCP)	tcp	995			
DNS(TCP)	tcp	53			
DNS(UDP)	udp	53			
ICQ	udp	4000			
SQL	tcp	3389			
1433	tcp	1433			
APPsoft	udp	3000	3000	4000	提交 重置

图 4-70：定义服务对象

2. 添加服务对象组

当希望对某个主机、主机组或者子网进行多个相同服务访问控制，或者将要限制的某些服务是由多个协议组成时，可以将这些服务添加到一个服务对象组里。

例如：允许局域网主机都可以收发来自任何地方的邮件。

首先定义邮件服务，众所周知 Web 邮件服务主要用到 POP3、STMP、DNS、HTTP 等协议，如下图界面，点击"新建服务对象组"，设置组名称 Mail。



服务对象组

组名称	编辑
Mail	
	新建服务对象组

合计已定义: 1 个服务对象组

图 4-71：新建服务对象组

接着为 Mail 添加组成员，点击"新建服务对象组"添加服务对象成员，具体设置如下图示：



服务对象组：Mail

服务名称	编辑
HTTP	
SMTP	
POP3	
DNS(TCP)	
HTTP	提交 重置

图 4-72：添加服务对象成员

删除组或其成员，点击删除“”删除组成员，但要注意，当一个服务被访问控制规则引用时，必须先删除控制规则。

时间对象管理

制定基于时间计划的防火墙控制规则，需事先设置时间计划对象。

如下图示，在时间对象列表可以进行时间对象管理如添加新对象、删除对象及修改对象。

时间对象

时间对象名称	开始时间	结束时间	星期	编辑
onduty	08:00	11:00	0,1,2,3,4,5,6	
offduty	12:00	14:30	1,2,3,4,5	

添加

图 4-73：时间对象

添加一个新的时间计划，在时间对象列表里点击“添加”进入设置界面，如图示：

新时间对象

对象名称							
开始时间	时		00	分		00	
结束时间	时		00	分		00	
日	日	一	二	三	四	五	六
选择	☑	☑	☑	☑	☑	☑	☑

提交

图 4-74：新加服务对象

- ☑ 对象名称： 设置时间计划标识，有效字符 1-32 位大小写英文、数字或其组合。
- ☑ 开始时间： 时间计划的起始时间，时：0~24、分：00、15、30、45、59。
- ☑ 结束时间： 时间计划的结束时间，时：0~24、分：00、15、30、45、59。
- ☑ 日期选择： 周一至周五的任意时间组合。

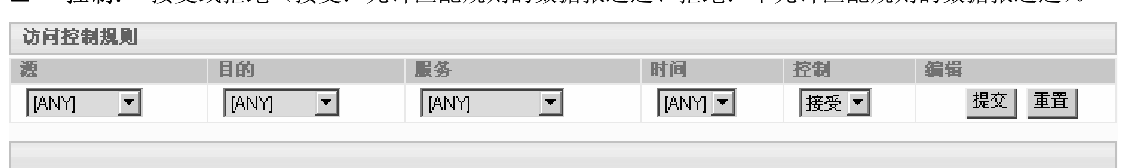
注意：

由于系统时间对象的开始时间不能大于结束时间，所以如果要设置结束时间为晚上零点，则必须设置为 23:59

访问控制规则管理

基于源地址、目的地址、服务端口和协议的访问控制管理设置如下：

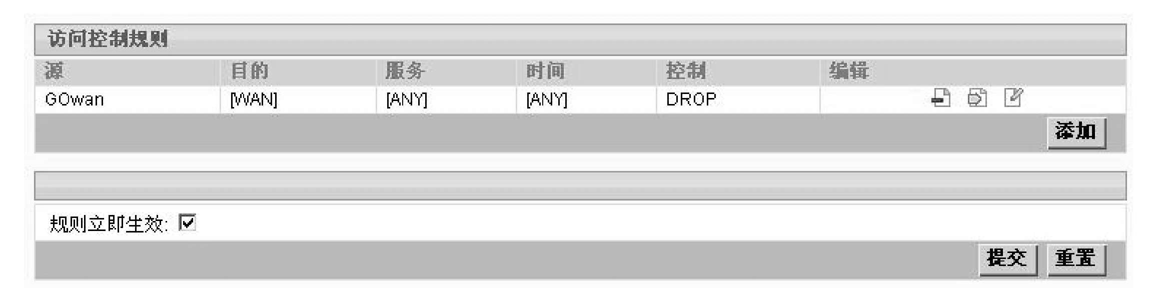
- ☑ 源： 数据报发送端（节点、节点组、子网）。
- ☑ 目的： 数据报接受端（节点、节点组、子网）。
- ☑ 服务： 需要控制的服务对象（服务对象、服务对象组）。
- ☑ 时间： 时间计划对象。
- ☑ 控制： 接受或拒绝（接受：允许匹配规则的数据报通过、拒绝：不允许匹配规则的数据报通过）。


访问控制规则

源	目的	服务	时间	控制	编辑
[ANY]	[ANY]	[ANY]	[ANY]	接受	提交 重置

图 4-75：访问控制规则表

例如：添加拒绝节点组 GOwan 在 ANY 时间上网的控制规则。具体如下：



访问控制规则

源	目的	服务	时间	控制	编辑
GOwan	[WAN]	[ANY]	[ANY]	DROP	

添加

规则立即生效: ☑

提交 重置

图 4-76：添加访问控制规则

在某条规则前插入一条规则时，点击该规则编辑栏“”即可进入插入状态进行新规则设置，修改规则点击“”。删除一条规则点击其后的“”即可删除。

注意：

❶ 防火墙规则执行是按照控制列表顺序从上到下执行的，所以设置防火墙规则必须考虑规则间的互相关联及限制

❷ 添加多条防火墙规则时，建议取消“规则立即生效”设置，否则会减慢规则保存速度

NAT/PAT

(一) 目的地址转化

目的地址转换简单的说就是指将内网服务器映射到设备外网口公网 IP 地址上，即 IP+Port 的映射，一般用于对外部隐藏服务器地址，不但可以保证服务器安全还可以节省公网 IP 地址资源。

☑ **目的**：指设备外网口 IP 地址。

☑ **服务**：是内部服务器所提供的服务。

☑ **进入接口**：数据进入设备的硬件接口。

☑ **转换后目的**：内部真正提供服务的主机 IP 地址。

☑ **转换后服务**：内部服务器服务端口，须于”**服务**”设置相同，不可重定向。



目的地址转换

目的	服务	进入接口		转换后目的	转换后服务	编辑
Wanip	HTTP	[ANY]	--->	server	HTTP	
aaa	[ANY]	[ANY]	--->	aaa	[ANY]	提交 重置

图 4-77：目的地址转换列表

(二) 目的地址映射

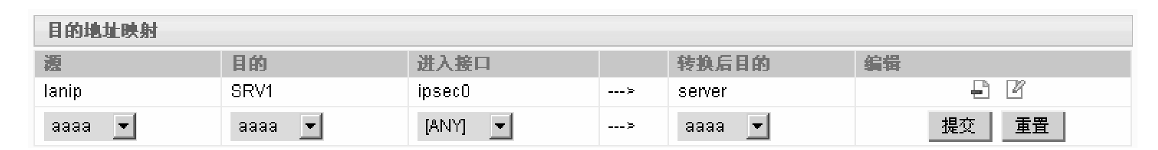
目的地址映射是指将通过设备并进入内网的数据报目的 IP 地址映射为内网里另一台主机 IP 地址，和目的地址区别在于不需要做服务映射。

☑ **源**：发出访问请求的 IP 地址。

☑ **目的**：访问的目的 IP 地址。

☑ **进入接口**：数据进入设备的硬件接口。

☑ **转换后目的**：真正提供服务的主机 IP 地址。



目的地址映射

源	目的	进入接口		转换后目的	编辑
lanip	SRV1	ipsec0	--->	server	
aaaa	aaaa	[ANY]	--->	aaaa	提交 重置

图 4-78：目的地址映射列表

(三)源地址转换

源地址转换是指将通过从设备转发的数据报源 IP 及服务映射至设备的外出端口上。

☑ **源：**发出访问请求的 IP 地址。

☑ **目的：**访问的目的 IP 地址。

☑ **服务：**是内部服务器所提供的服务。

☑ **外出接口：**数据外出设备的硬件接口。

☑ **转换后源：**映射后的源 IP 地址。



源地址转换

源	目的	服务	外出接口	转换后源	编辑
lannet	server	HTTP	ixp0	lanip	
[ANY]	[ANY]	[ANY]	[ANY]	aaa	提交 重置

图 4-79：源地址转换列表

注意：接口说明
eth0 或 ixp1 指内网口；eth1 或 ixp0 指外网口；ANY 指代所有接口；ppp0 是指 PPPOE 拨号接口，当外网线路为 ADSL 时，可以选择此接口作为数据外出/进入接口；ipsec0 是指 VPN 隧道数据传输接口，当数据需要通过隧道传输时选择该接口，建议在无法确认时选用 ANY.

防 ARP 攻击

ARP "Address Resolution Protocol"（地址解析协议），在局域网中 ARP 协议的基本功能是通过目标设备的 IP 地址查询其 MAC 地址以保证通信的顺利进行。ARP 协议对网络安全具有重要的意义，而 ARP 病毒攻击则常常会导致网络时断时续或者不可用等异常，该病毒主要通过对内网的计算机进行攻击，以伪造 IP 地址和 MAC 地址实现 ARP 欺骗，致使内网计算机的 ARP 表混乱，并在网络中产生大量的 ARP 通信量造成网络阻塞。因此通过预防措施来避免 ARP 病毒是防患于未然的必要手段。

APN 设备通过 ARP 广播及 IP 和 MAC 绑定的方式来预防内网 ARP 病毒感染。

ARP 广播

设备 ARP 广播是指设备系统在一定的时间间隔向内网发送 IP 报文广播，管理员可以通过调节设备的广播速率来控制 ARP 病毒广播，当设备广播速率远远大于 ARP 病毒广播时就可以达到控制目的了。缺省情况下，系统会每隔 20 秒发送一次广播。

如下图示，设置好广播时间间隔后，勾选"启用 ARP 广播"即可生效。

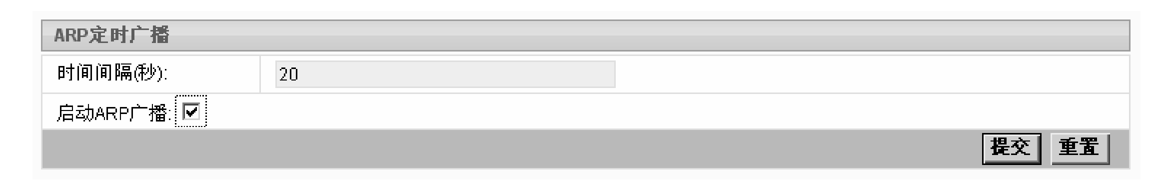


图 4-80：ARP 广播设置

MAC 地址邦定

MAC 绑定设置，即将主机 IP 与其 MAC 地址绑定设置。

一般情况下，设备会通过 ARP request 来动态获得内网计算机 IP 跟网卡地址的对应，并且在设备的 ARP 表中增加相应的纪录。当内网有 ARP 欺骗行为时，可能会导致设备动态获得的计算机 IP 跟网卡地址对应不正确。为了避免这种情况发生，可以在设备进行 MAC 地址绑定设置，如下图示：

MAC与IP绑定

IP地址	MAC地址	编辑
192.168.138.25	00:FF:03:7E:E8:25	
192.168.138.110	00:FF:08:EA:D5:49	

添加

图 4-81：MAC 与 IP 绑定

- ☑ **IP 地址**：指定的 IP，格式：xx.xx.xx.xx。
- ☑ **MAC 地址**：制定 IP 对应的网卡地址，有效格式必须为：XX:XX:XX:XX:XX:XX。

“删除”已绑定的 IP 和没 MAC 绑定设置即可解绑。再次邦定需要重新添加。

攻击防范

攻击的法律定义是：攻击仅仅发生在入侵行为完全完成且入侵者已在目标网络内。但是更积极的观点是（尤其是对网络安全管理员来说）：可能使一个网络受到破坏的所有行为都应称为攻击。即从一个入侵者开始在目标机上工作的那个时刻起，攻击就开始了。

通常，在正式攻击之前，攻击者都会试性攻击，目的是获取系统更有用的信息，例如：ping 扫描，淹没式和 Denial of Service 式的攻击等等，像这样的攻击经常会导致网络出现拥塞现象、服务器停止服务或死机。那么开启"防范 Ping-of-death"、"防同步洪水"设置显得很必要，如下图示：

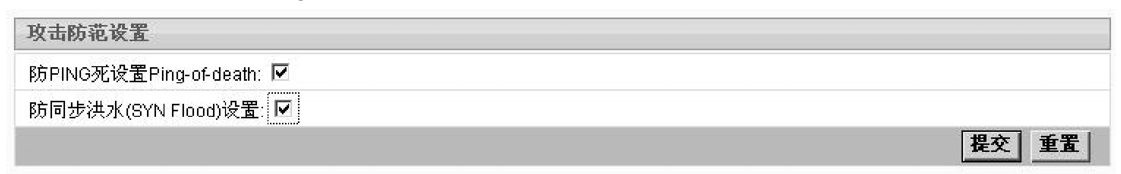


图 4-82：攻击防范设置

带宽管理

设备支持带宽管理 TC (流量控制，Traffic Control)模块。该模块支持优先、共享和输入、输出流量限制等。本节将讨论如何使用设备来有效的管理有限带宽。

基本概念

设备带宽管理功能由基本设置、带宽策略及带宽规则三部分组成，**设置顺序为：基本设置→带宽策略→带宽规则**，即设置的思路是先定义总带宽，再详细定义带宽策略，然后把定义好的策略应用于不同的规则之中。

带宽管理功能主要是设置通过设备的数据包流量和优先等级，实现对用户本地网络有限带宽的上行和下行进行按需应用的合理管理。

- ☑ 上行： 设备内部网络向外网或者对端网络发送数据包，为上行；
- ☑ 下行：外部网络或者对端网络往 设备内部网络发送数据包，为下行。

例如：局域网的一台 PC 机从互联网的一个 FTP 服务器上下载一个软件，是属于下行还是上行呢？

下行。

因为主要的数据是由外部的 FTP 服务器流向局域网的 PC 机的。

再如： 设备内部的一台数据库服务器对对端的 PC 提供数据，这时，是属于下行还是上行？

上行。

因为主要的数据是由局域网的数据库服务器流到对端网络的 PC（数据库客户端软件）。

如下图示：

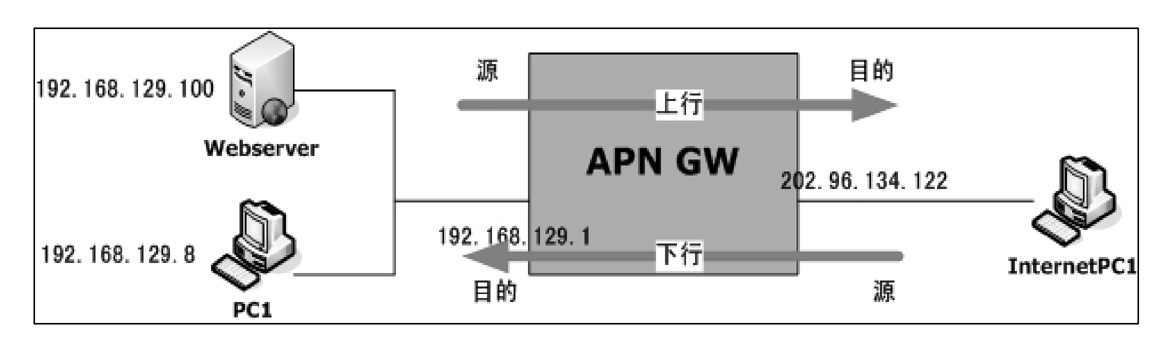


图 4-83：上下行带宽图示

基本设置

基本带宽设置要求根据上网线路的实际上下行总带宽设置对应总带宽。例如，当使用 ADSL 上网线路时，这里设定上行总带宽为 512Kbps，下行总带宽为 2048Kbps，可以略小于实际带宽设置。如图示：

基本带宽设置	
上行总带宽(kbps):	500
下行总带宽(kbps):	2000
	提交 重置

图 4-84：带宽管理基本设置

带宽策略

定义了带宽值之后，接下来需按照本地局域网总带宽应用情况来分配带宽，并进行定义多条带宽策略。带宽策略定义如下示：

带宽策略					
策略名称	带宽(kbps)	优先级	限制	方向	编辑
fileUP	200	1	限制	上行	
fileDOWN	100	8	不限制	下行	
					添加

图 4-85：带宽策略定义

☑ **策略名称**：可以是字母和数字的组合，最好包括"down"和"up"表示上行还是下行的策略。

☑ **带宽**：需要限制的带宽。

☑ **优先级**：策略的优先级分为 1-8。优先级高的数据包被优先发送，其中"1"为优先级最高，"8"为最低。

☑ **限制**：是否允许借用空闲的带宽。当设置为"限制"时，匹配此策略的数据只能以设定的最大带宽发送，否则可以借用其他空闲的带宽。

☑ **方向**：选择此策略由上行数据还是下行数据来匹配。设置为"上行"时，此策略应用于外网口；设置为"下行"时，此策略应用于内网口。

带宽规则

带宽规则是带宽策略的具体应用设置。如下图示，一个带宽规则的主要参数包括：

带宽规则						
源IP	源端口	目的IP	目的端口	协议	策略	编辑
192.168.138.25	any	0.0.0.0/24	21	tcp	fileDOWN	
192.168.138.235	any	211.152.9.59	21	tcp	fileUP	
						添加

图 4-86：带宽规则定义

☑ **源 IP**： 数据包发出的源 IP 地址或网段，网段格式：IP 地址/掩码位数。例如要输入 192.168.100.0/255.255.255.0 的网段，就是 192.168.100.0/24。未输入掩码位数时，系统默认为 32 位，代表一台主机。

☑ **目的 IP**： 数据包到达的目标 IP 地址或网段。0.0.0.0/0 表示到所有网络。

☑ **源端口**： 数据包服务类型。比如，Web 服务端口为 80。空代表<ANY>，指网络上的任意服务。

☑ **目的端口**：同源端口定义。

☑ **协议**： 数据协议类型 TCP 或 UDP。

☑ **策略**： 已定义的上下行策略，按照实际数据传输需求引用。

点击"添加"可以添加新的带宽应用规则，删除一条已有规则点击" "，如果要在某条规则前插入一条规则点击插入" "。

注意：如果这里选择了"ANY"，则不需要设置"源端口"和"目的端口"

流量监控

流量监控的主要功能是为了监控内部上网各种流量情况，及会话连接情况等，其功能设置包括：

基本设置

启动“网络监控”服务就可对局域网进行上网流量及会话连接监控及查看，打开服务 5 分钟后就可以看到统计结果。

如下图示：进入“基本设置”勾选“启动网络监控”，并“提交”将成功打开网络监控。

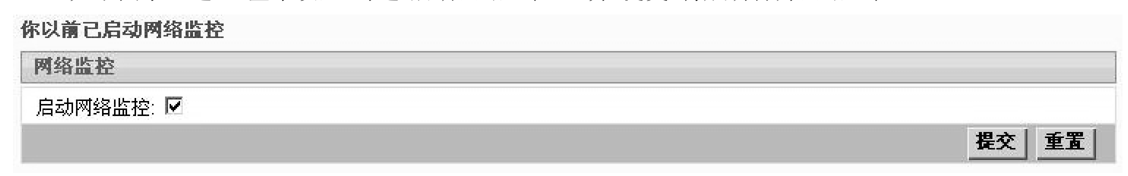


图 4-87：启动网络监控

网络传输

网络传输主要用于统计各种数据包协议流量，是按照每 5 分钟累计一次通过设备的数据总流量（M）和各协议流量来统计的。如下图示：

网络传输表

Host	Total	Total Sent	Total Recv	5Min Total	5Min Sent	5Min Recv	TCP	UDP	ICMP	OTHER
Total	386.4K	145.5K	240.9K	386.4K	145.5K	240.9K	377.7K	8.7K	0	0
192.168.138.180	295.4K	92.9K	202.6K	295.4K	92.9K	202.6K	286.8K	8.7K	0	0
192.168.138.1	90.9K	52.6K	38.3K	90.9K	52.6K	38.3K	90.9K	0	0	0

图 4-88：网络传输

更为详细的统计曲线分析图统计查看，可点击表中 HOST 列中主机 IP，可查看到具体主机的协议流量分布图：Last 60 Minutes Tracffic、Last 24 Hours Tracffic、Last 30 Days Tracffic 以及 TCP/UDP 传输端口分布表（最近几分种）等等详细情况，60 分钟流量图是每 5 分钟的流量，单位为字节。如下图示：

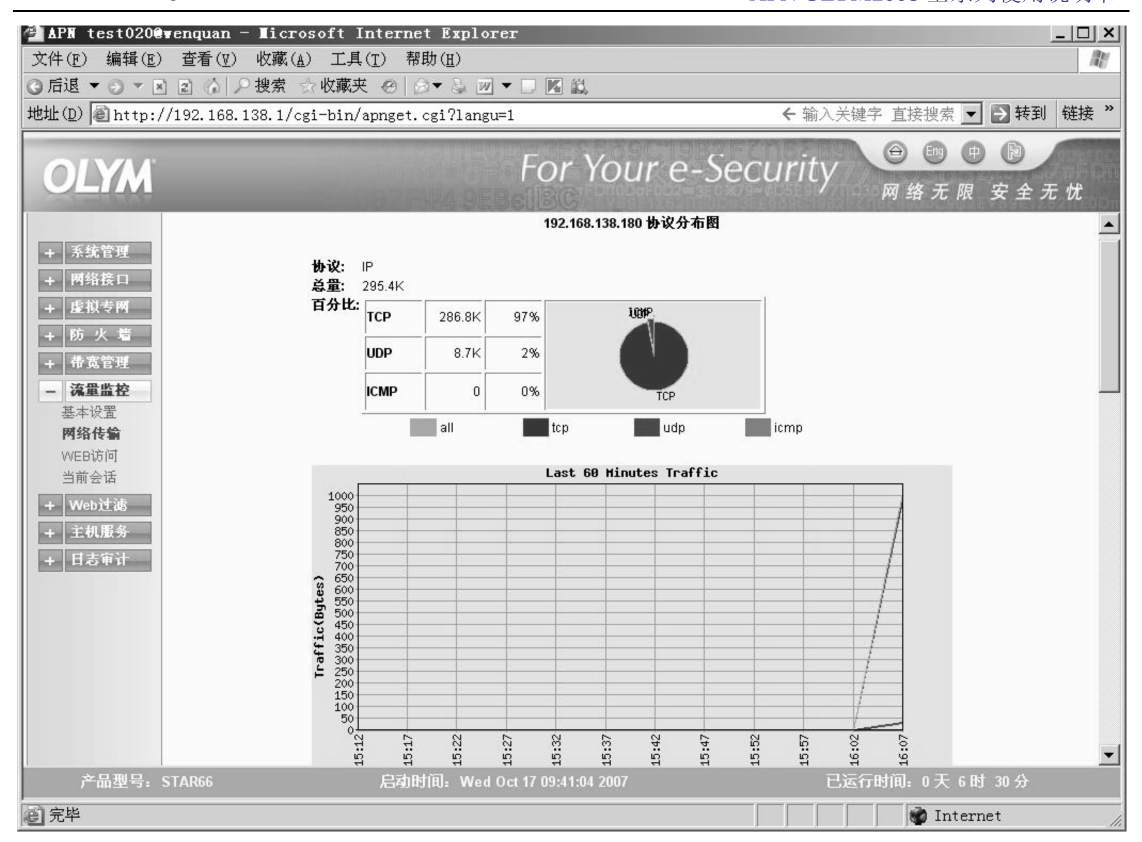
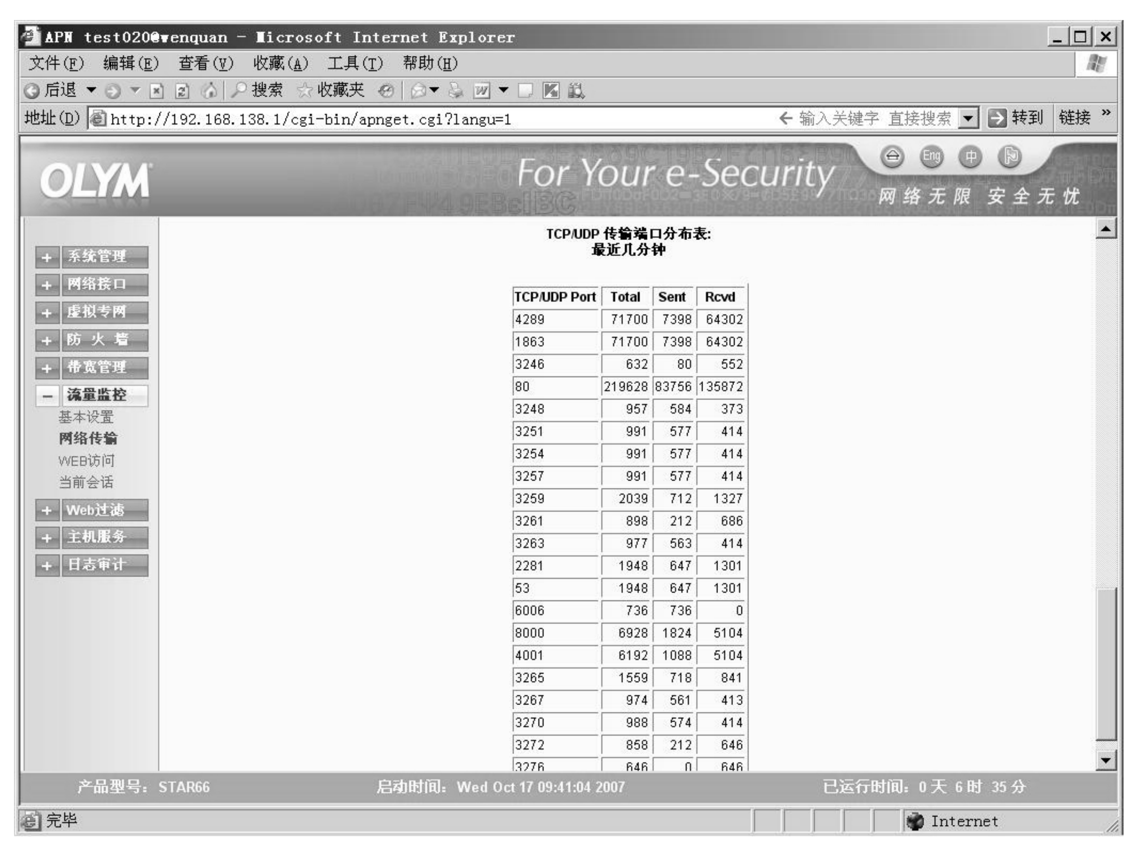


图 4-89：协议分布统计图



TCP/UDP 传输端口分布表:
最近几分钟

TCP/UDP Port	Total	Sent	Rcvd
4289	71700	7398	64302
1863	71700	7398	64302
3246	632	80	552
80	219628	83756	135872
3248	957	584	373
3251	991	577	414
3254	991	577	414
3257	991	577	414
3259	2039	712	1327
3261	898	212	686
3263	977	563	414
2281	1948	647	1301
53	1948	647	1301
6006	736	736	0
8000	6928	1824	5104
4001	6192	1088	5104
3265	1559	718	841
3267	974	561	413
3270	988	574	414
3272	858	212	646
3276	646	0	646

图 4-90：TCP/UDP 传输端口分布表



Web 访问

如下图示，Web 访问列表列出本地局域网内每台主机上网浏览网页的情况：访问时间、访问 URL，网络管理员可以据此了解局域网内常常访问资源情况并进行很好的网络管理。

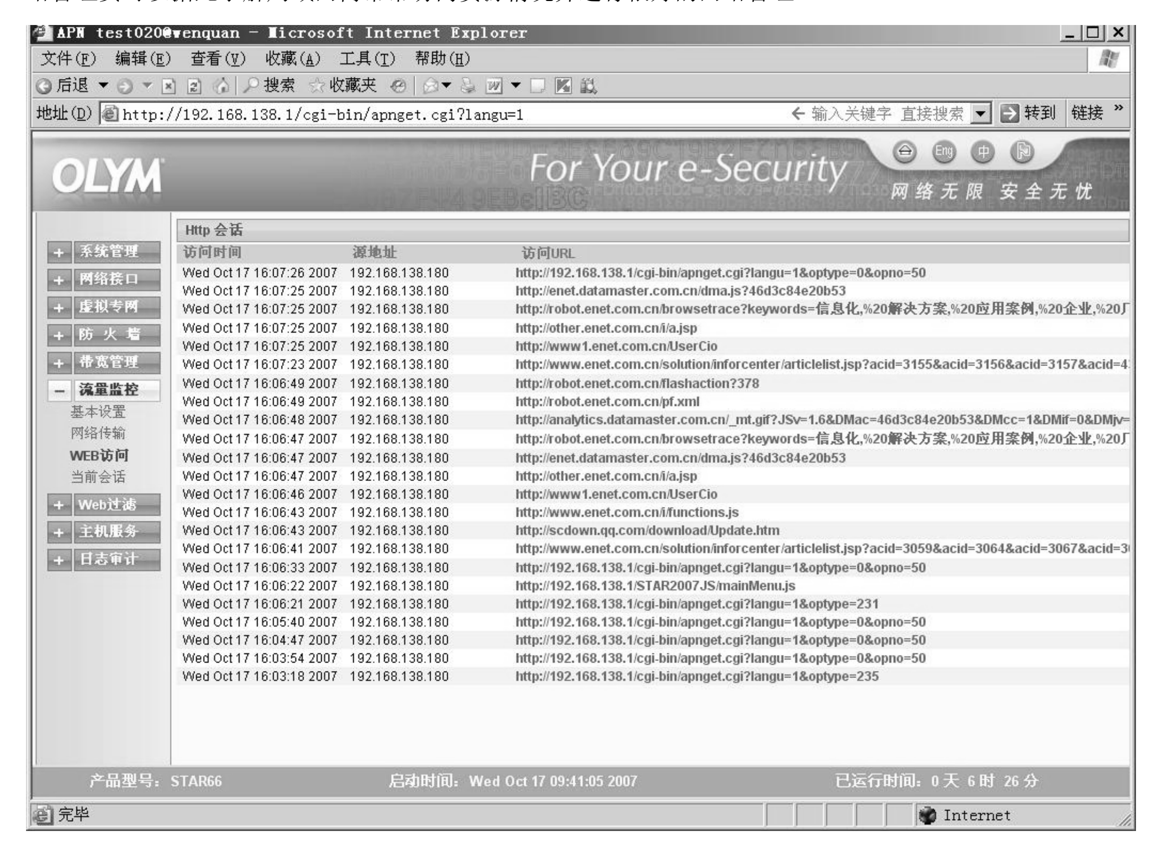


图 4-91：HTTP 会话

注意：

❶ 流量监控抓取内网口的所有数据包，缺省情况下只把源地址或者目的地址属于内网接口 IP 网段的数据包进行记录分析。其他网段不做记录。

❷ 流量监控数据是以字节为单位统计分析并记录。

❸ 每次设备重启，系统都会清除磁盘所有统计记录。有必要敬请做好备份。

当前会话

设备当前会话是通过记录不同协议（TCP、UDP、ICMP）数据包的 Sorce（源地址）、Destination（目的地址）、State（连接状态）、Sport(源端口)、Dport（目的端口）等的数据包情况，依据这些记录可以判断网络是否存在异常，比如当发现在 TCP 和 UDP 会话里 Dport 出现很多 135、136、137、138、139、445 等等端口，就可定位局域网内可能有蠕虫等病毒，同时根据源地址则可定位到具体的计算机。

(一) TCP 会话查看

如下图示，通过 TCP 会话列表可以看到任何通过系统得 TCP 会话连接情况

TCP 会话

Source	Destination	State	Sport	Dport
192.168.138.180	116.254.174.4	TIME_WAIT	4016	8000
192.168.138.180	116.254.174.4	TIME_WAIT	4008	8000
192.168.138.180	116.254.174.4	TIME_WAIT	4026	8000
192.168.138.180	192.168.138.1	ESTABLISHED	4028	80
192.168.138.180	192.168.138.1	TIME_WAIT	4012	80
192.168.138.180	219.133.60.243	ESTABLISHED	1991	8000
192.168.138.180	81.52.202.54	TIME_WAIT	3940	80
192.168.138.180	116.254.174.4	TIME_WAIT	4018	8000
192.168.138.180	192.168.138.1	TIME_WAIT	4014	80
192.168.138.180	192.168.138.1	TIME_WAIT	4004	80
192.168.138.180	60.21.99.171	ESTABLISHED	4361	26574
192.168.138.180	192.168.138.1	TIME_WAIT	4006	80
192.168.138.180	207.46.106.17	ESTABLISHED	4289	1863
192.168.138.180	116.254.174.4	TIME_WAIT	4024	8000
192.168.138.180	192.168.138.1	TIME_WAIT	4020	80
192.168.138.180	116.254.174.4	TIME_WAIT	4010	8000

图 4-92：TCP 会话列表

(二) UDP 会话查看

像 TCP 会话列表一样，UDP 会话列表也详细显示了通过系统所有当前 UDP 会话连接情况。

UDP 会话

Source	Destination	Sport	Dport
192.168.131.25	10.0.0.152	1183	8401
192.168.131.25	10.0.0.152	1181	8401
192.168.131.25	10.0.0.152	1182	8401
192.168.138.180	219.133.41.73	4001	8000
192.168.131.91	192.168.131.255	138	138
192.168.131.25	10.0.0.152	1179	8401
192.168.131.25	10.0.0.152	1185	8401

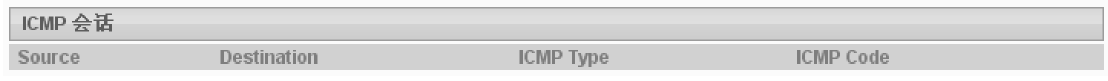
图 4-93：UDP 会话列表

(三) ICMP 会话查看

ICMP 协议虽然不像 TCP 和 UDP 是传输用户数据报协议。但对于用户数据的传递起着重要作用。并对网络安全具有极其重要的意义。其本身特点决定了它非常容易被用于攻击网络上的路由器和主机。

例如：黑客们可能会利用操作系统规定的 ICMP 数据包最大尺寸不超过 64KB 这一规定，向主机发起“Ping-of-death”攻击。此外，大量的 ICMP 数据包会形成“ICMP 风暴”，使得目标主机耗费大量的 CPU 资源，疲于奔命。

如下图示，系统提供 ICMP 会话查看，通过 ICMP 会话查看可以有效预防基于 ICMP 协议的威胁攻击。



ICMP 会话

Source	Destination	ICMP Type	ICMP Code

图 4-94：ICMP 会话列表

Web 过滤

Web 过滤用于过滤内部主机对 Web 服务器的 HTTP 请求，并使用预先定义的规则允许和禁止其连接， 设备支持以下过滤设置：

URL 过滤

URL 过滤可以禁止内网访问一些非法的、色情的、蛊惑的、以及公司限制网站/页等等。URL 过滤包括：URL 黑名单和 URL 白名单，如下图示：

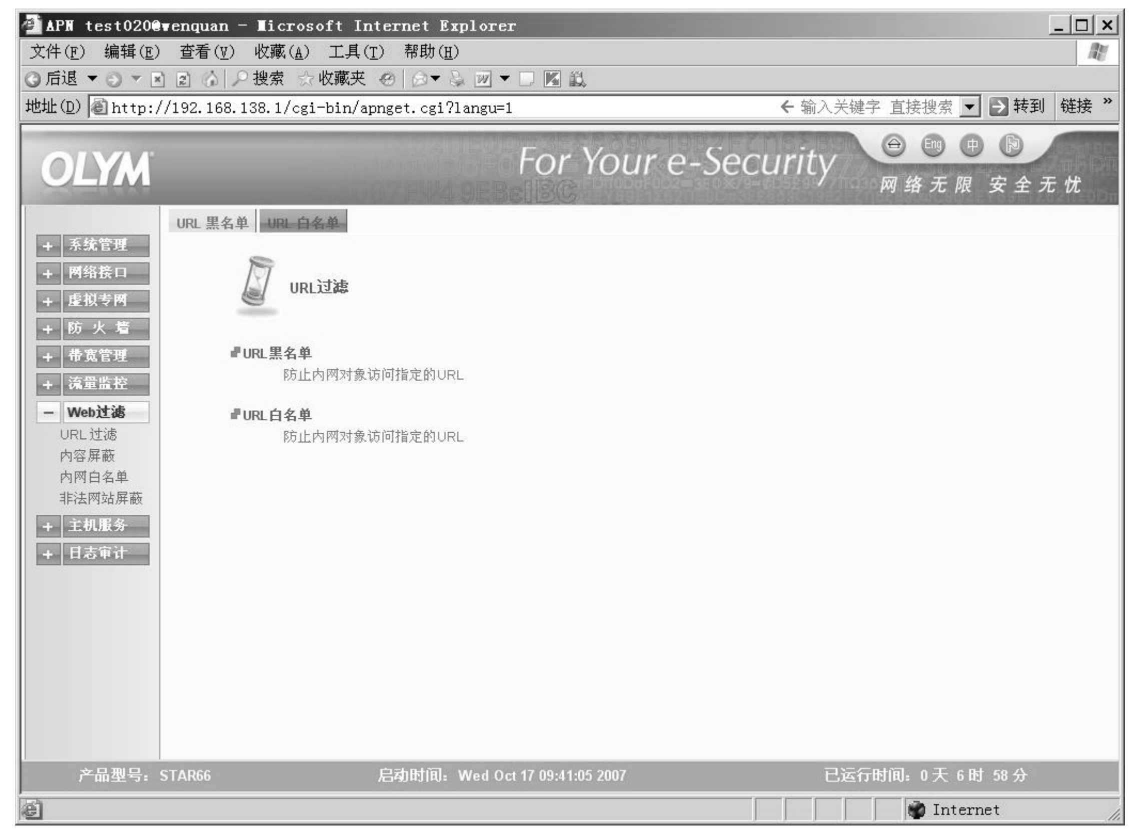


图 4-95：URL 过滤

(一)　URL 黑名单设置

进入"URL 黑名单"配置界面，单击"添加"根据控制需求进行黑名单添加管理。

例如：限制all_net对网站www.chat.com进行访问，首先请定义要控制的对象名称（请参考防火墙"网络对象管理"设置）。



URL屏蔽列表

网络对象	URL	编辑
all_net	www.chat.com	
all_net	www.qq.com	
BOb	www.msn.com	
John	***	

添加

图 4-96：URL 屏蔽列表

完成设置后"提交"立即生效。删除某个控制规则，点击编辑栏" "按钮即可删除。

注意：

❶ 进行 URL 屏蔽设置须先设置定义网络对象，敬请参考"防火墙"部分

❷ URL 名称可使用通配符，如屏蔽新浪、网易等网站的所有 URL 链接，。可以输入：*sina*、*163*

等。

❸ 当要屏蔽所有网站，设置 URL 为“***”

(二) URL 白名单设置

URL白名单即URL免屏蔽设置，允许某个主机、网络或主机组访问一些网站。例如：在URL屏蔽已经屏蔽了网易所有网站的URL（*163*），但是又允许内网访问chat.163.com、mail.163.com，则可以将其列为免屏蔽列表内容

URL免屏蔽列表

网络对象	URL	编辑
all_net	www.apn.com.cn	
all_net	www.olymtech.net	
administrator	www.sina.com	
all_net	chat.163.com	
all_net	mail.163.com	

添加

图 4-97：URL 免屏蔽列表

内容屏蔽

内容屏蔽及关键字屏蔽，当前设备支持英文、数字、及其组合的关键字屏蔽。

例如：禁止局域网对含有“sex”相关内容的网页/网站进行访问查看，设置如下图示：

Web内容屏蔽

网络对象	关键字	编辑
all_net	aiuabin	
all_net	sexsex	
GOwan	njoamopdw	

添加

图 4-98：Web 内容过滤

删除一条内容屏蔽规则，点击该规则之后的“ ”即可删

注意： 关键字字符设置必须 3 个以上

内网白名单

内网白名单是对局域网内个别 IP 或网段不进行 Web 过滤限制，其优先级高于 URL 过滤和内容屏蔽。例如：免除 IP 为 192.168.138.25 的内部主机对 URL 的请求，设置如图示，点击 “添加”即可进行 IP 设置。



IP免屏蔽列表

IP地址	子网掩码	编辑
192.168.138.25	255.255.255.255	
192.168.138.235	255.255.255.255	

添加

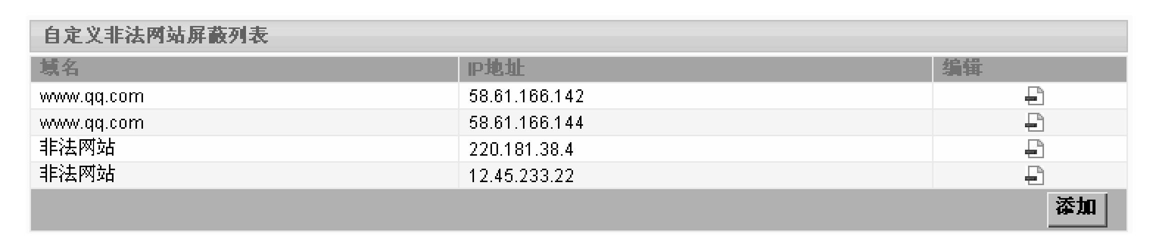
图 4-99：IP 免屏蔽

取消 IP 免屏蔽，点击“ ”撤销对此 IP 的限制。

注意：IP 免屏蔽为具体 IP 地址时，其对应子网掩码必须设置为 255.255.255.255

非法网站屏蔽

例如：某企业将QQ网站作为非法网站限制员工上班时间浏览其上的大量信息。点击“添加”www.qq.com提交后系统会自动解析到QQ所有服务器地址。如下图示，当管理员只知道某非法网站的IP地址，也可以直接添加IP地址，则系统将其域名显示为”非法网站”


自定义非法网站屏蔽列表

域名	IP地址	编辑
www.qq.com	58.61.166.142	
www.qq.com	58.61.166.144	
非法网站	220.181.38.4	
非法网站	12.45.233.22	

添加

图 4-100：非法网站屏蔽列表

删除一条屏蔽规则，点击该规则编辑栏“ ”即可删除。

注意：当屏蔽非法域名时，请确认已经启用“主机服务”的“DNS 服务”。

主机服务

设备主机服务集成了基本上网管理所用到的服务：远程登陆、WEB 服务、SNMP 服务、域名服务、动态 IP 分配、动态域名服务、双机热备份、MAC 地址绑定等服务。

远程登录

Telnet 服务常用于网络设备的远程协助管理和调试。该功能缺省情况下是关闭状态，如下图：



图 4-101：Telnet 服务

警告： 打开 telnet 功能预示着获得更多设备系统信息，强烈建议修改初始密码。

WEB 服务

WEB 服务缺省端口为 80。为了使用 80 端口带来安全隐患，设备支持 Web 服务端口修改。如下图示：

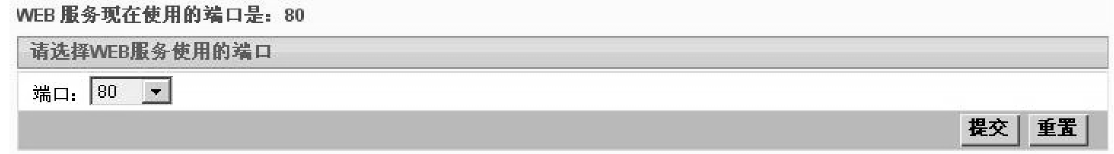


图 4-102：WEB 服务

注意：例如将 Web 端口修改为 8080 后，当通过 Web 管理界面再次进行配置管理时，需要使用格式 **http:192.168.32.200:8080/**进行访问

SNMP

启用 SNMP 代理，用户可以通过第三方的 SNMP 工具监控设备接口流量，协议数据报流量，数据报分析等等。缺省的通信密码是 gw1admin，支持 SNMP v1、V2c 和 V3。

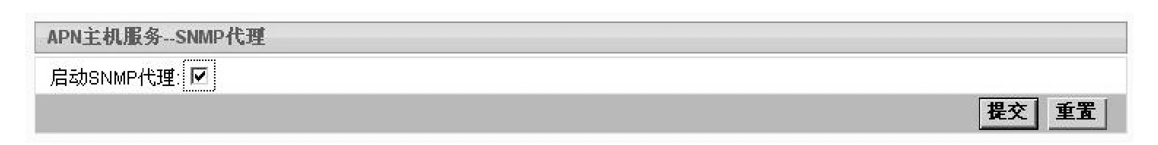


图 4-103：SNMP 代理服务

多播转发

多播(MultiCast)是一种点到多点(或多点到多点)的通信方式，即多个接收者同时接收一个源发送的相同信息。在网络中的主机若要接收发自一个特定组的多播报文，就要监听发往该特定组的所有报文。为了解决网络里多播报文的选路，主机须通过通知其子网上的多播路由器来加入一个组，多播中采用因特网组管理协议（IGMP）来达到此目的。

设备支持IGMP协议，当网络中有一台主机192.168.139.5和192.168.0.1需要加入 设备所在的多播组里进行接收广播，设置如图示：



图 4-104：多播转发设置

设置完成后选择启动多播转发功能，点击"提交"即可生效。

域名服务

DNS 代理服务功能可以代理内网进行 DNS 服务请求，在如下图示：

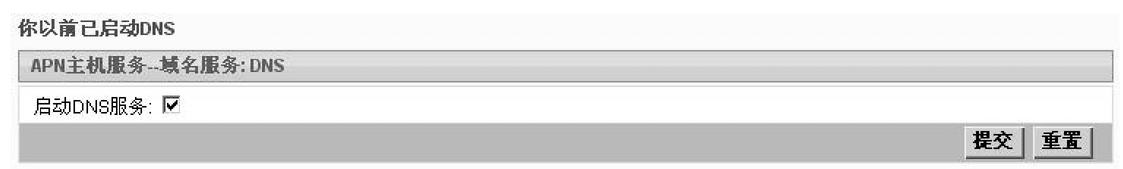


图 4-105：DNS 服务

动态 IP 分配

(一) DHCP 服务配置

如下图示，在开启 DHCP 服务前必须设置以下参数：

你以前已启动DHCP服务.
分配范围: 192.168.138.2 - 192.168.138.254

APN主机服务--动态地址分配服务:DHCP

分配起始地址:	192.168.138.2
分配终止地址:	192.168.138.254
可选网关:	192.168.138.1
可选DNS:	202.96.134.133
可选WINS:	
启动DHCP: ☑	

提交 重置

动态IP分配情况

IP地址	主机名

图 4-106：DHCP 设置

☑ **动态地址池**：分配起始地址和分配终止地址，由管理员根据网络 IP 地址规划来进行设置规定。
☑ **可选网关**：填写内网 IP 地址
☑ **可选 DNS**：可以是的内网 IP（必须启用域名服务功能），也可以是公网上 DNS
☑ **可选 WINS**：WINS 服务器地址设置
☑ **启动 DHCP**：设置完以上必要的参数后，开启启动参数才生效。

完成以上所有必需配置，要使服务设置被保存并生效，必须“提交”。

注意：

❶ 当不清楚本地当前具体的 DNS 地址,可以启动设备 DNS 代理服务进行域名解析服务请求。
❷ 如果使用电话拨号或是 ADSL 上网，并启动了的 DNS 服务时， DHC 则会自动把 PPP 对端的 DNS 服务器地址加入 DHCP 服务中。

(二) 动态地址分配查看

DHCP 已经分配的 IP 地址显示列表如下图示：

动态IP分配情况

IP地址	主机名

图 4-107：DHCP 地址分配查看

动态域名服务

客户在使用前必须先到www.3322.org 网站申请一个可用的域名，然后再进行动态域名设置。

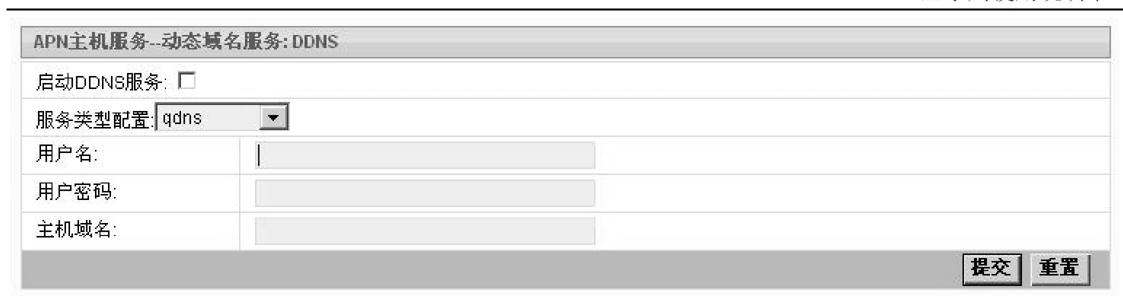


图 4-108：DDNS 服务配置

- ☑ **启动 DDNS 服务**：选中开启服务。
- ☑ **服务类型配置**：动态域名解析类型，建议是用缺省 qdns.
- ☑ **用户名**：在www.3322.org 上注册的帐号.
- ☑ **用户密码**：在www.3322.org 上注册的帐号对应的密码.
- ☑ **主机域名**：在www.3322.org 上申请的主机域名.

在启动服务前请按要求填写配置参数，同时注意服务类型配置采用默认即可。完成配置“提交”即生效。

双机热备份

设备支持 VRRP 协议实现双机热备功能，为网络提供高可用性保证。其实现是通过在网络中安装的两台互为主备关系的设备，当主设备出现故障时，备份设备主动承接主设备的工作，继续提供网络服务。

双机热备功能主要硬用于大型星型网络来增强网络高可用性，使用连接时外网可以是同一条专线的不同 IP 地址，或者是两条不同的外网线路，如两条 ADSL。

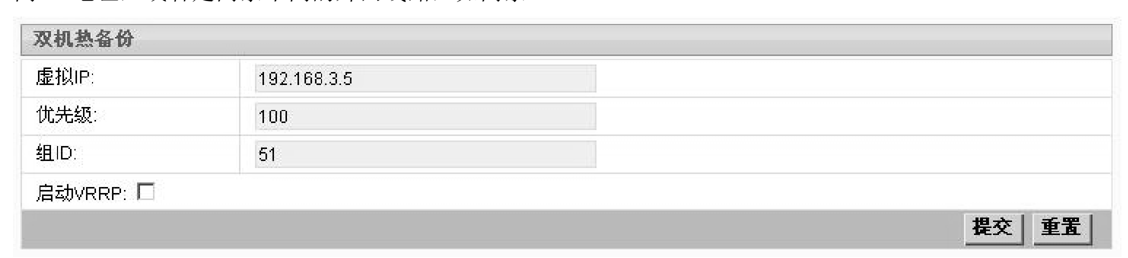


图 4-109：双机热备

- ☑ **虚拟 IP**：任意设置一个属于本地局域网 IP 段的没有被占用的 IP。互为热备份的设备的虚拟 IP 必须保持一致。
- ☑ **优先级**：优先级别按照数字的递增而增高，优先级范围：1-255。
- ☑ **组 ID**：是用来确定互为备份的设备的一个标识，所以所有热备份的设备都必须使用相同的 ID 号，取值范围为：1-100。
- ☑ **启动 VRRP**：开启 VRRP 双击热备功能。必须在配置完成后勾选并“提交”。

日志审计

日志审计功能包括：系统日志、VPN 日志、移动用户日志、日志配置等功能。

日志对于安全管理来说非常重要，其记录了系统实时运行及各种事件情况，可通过日志反映来判断系统故障发生的原因，或者受攻击时攻击者留下的痕迹。日志的主要功能是审计和监测，可以实时监测系统状态，追踪侵入者的入侵活动等等。

日志文件属于纯文本文件，每一行则为一个消息。每个消息都由四个域的固定格式组成：

- **时间标签(Timestamp)**：表示消息发出的日期和时间。
- **主机名(Hostname)**：表示生成消息的设备的名字。
- **生成消息的子系统的名字**：可以是“Kernel”，表示消息来自内核或者是进程的名字，表示发出消息的程序的名字。在方括号里的是进程的 PID。
- **消息(Message)**：即消息的内容。

系统日志

系统日志反映了系统运行中的所有进程调用情况，通过系统日志分析设备是否正常运行或者运行过程中的故障原因。

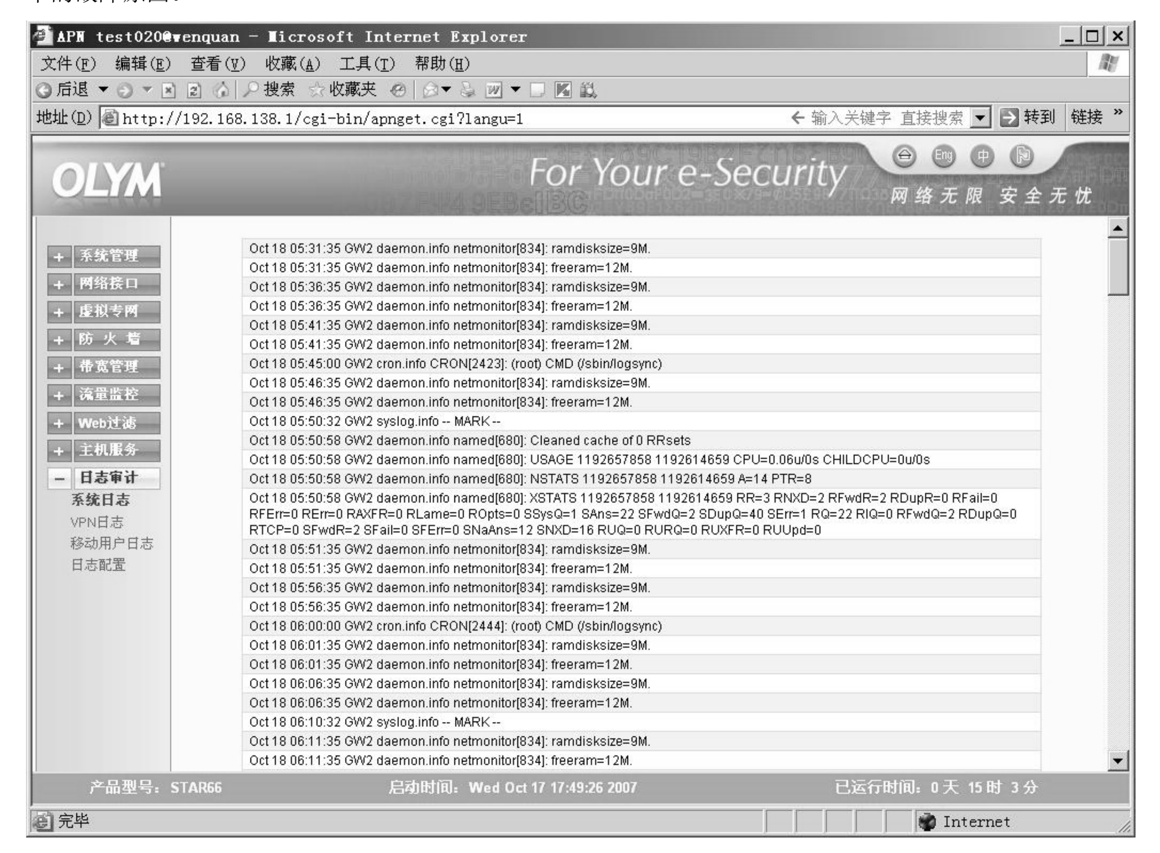


图 4-110：系统日志

VPN 日志

VPN 日志用于查看关于 VPN 隧道启动、停止和心跳检查的日志。通过 VPN 日志，可以准确地判断出节点在进行 IKE 协商过程中的异常，对于维护隧道起到很有效的作用。

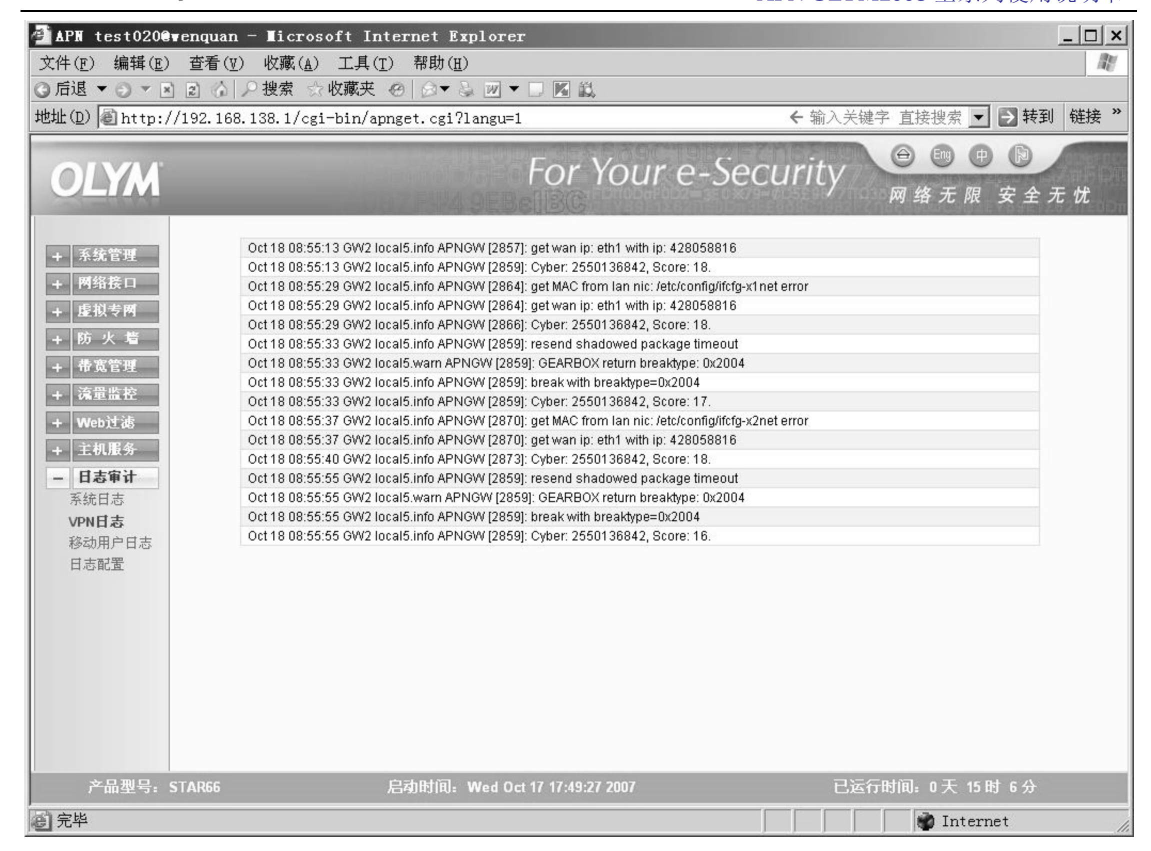


图 4-111：VPN 日志

移动用户日志

移动客户端日志记录了客户端通过远程拨入网络的情况，通过该日志的查看，可以及时准确了解客户端在接入过程中的问题，对于解决客户端接入异常判断检查很有帮助。

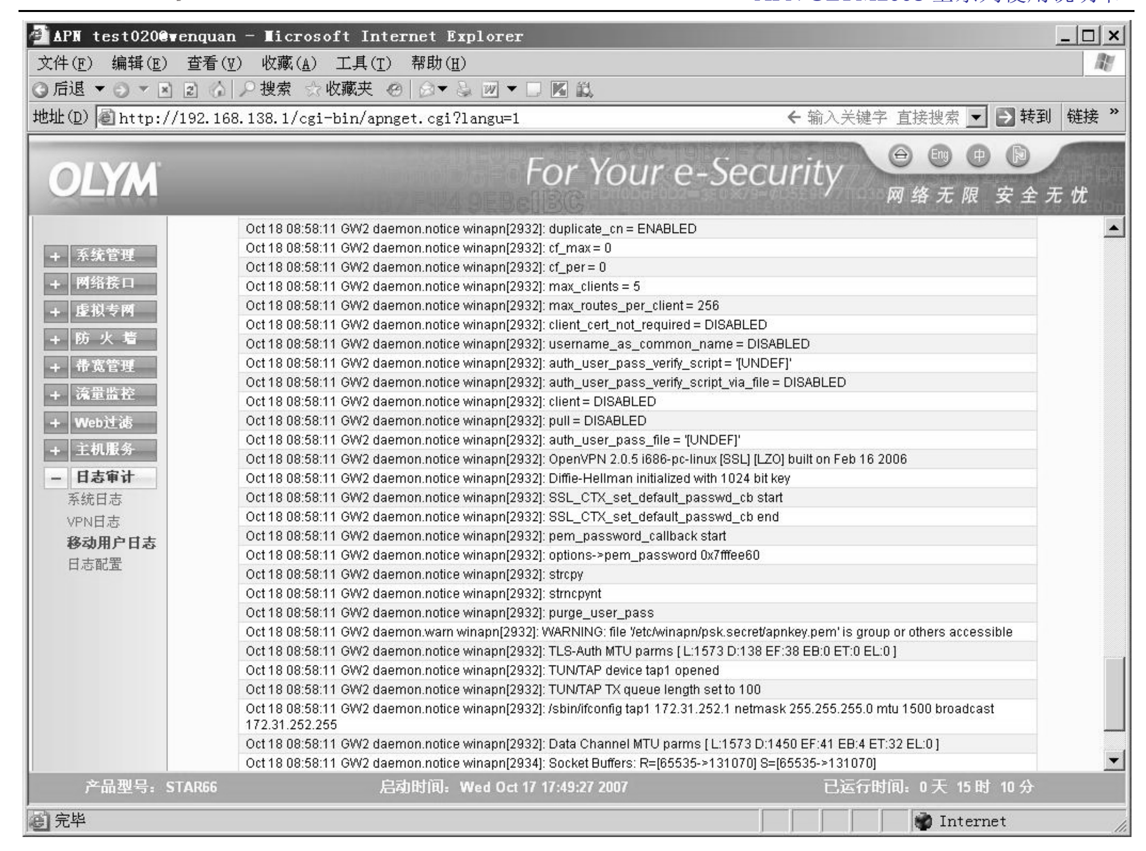


图 4-112：移动客户端日志

日志配置

日志配置功能提供给了用户进行日志管理的两种位置选择，缺省情况下，日志是记录在本机上的，即设备存储器内，用户可以根据需要把日志保存在远程日志服务上，来进行日志查看和管理，另外由于日志存储空间有限，因此进行远程日志管理可以保存所有的历史记录。



图 4-113：日志配置

如果选择存储在远程日志服务器上，那么必须事先确认远程日志服务器已经配置完成，然后再设置日志审计功能："使用远程日志服务器"，如下图示：

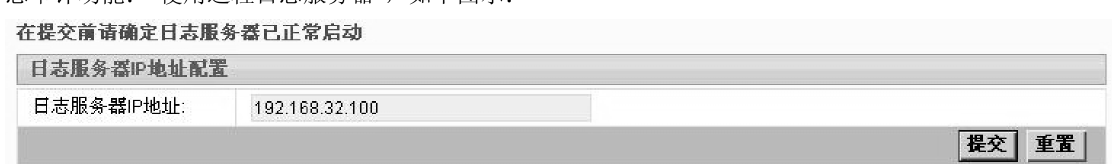


图 4-113：日志服务器配置

在"日志服务器 IP 地址"处填写设置好的远程日志服务器的 IP 地址，"提交"即可设置完成，重启设备后服务配置生效。

注意：日志服务器可以使用 3com公司的logserver软件来配置，软件下载地址www.olymtech.net 。

日志审计附加内容

日志构成：是由两个域组成，分别是“选择器(Selector)”和“动作(Action)“。“选择器”用相应的“设备”和“优先级”(都可以用”*”通配符表示”任何一个”)来表示消息的类型。“动作”表示一旦有一个新的消息和“选择器”相匹配时候要采取什么行动。

每个 syslog 消息被赋予下面的主要设备之一：

LOG_AUTH--认证系统：login、su、getty 等

LOG_AUTHPRIV--同 LOG_AUTH，但只登录到所选择的单个用户可读的文件中

LOG_CRON--cron 守护进程

LOG_DAEMON--其他系统守护进程，如 routed

LOG_KERN--内核产生的消息

LOG_SYSLOG--由 syslogd（8）产生的内部消息

Syslog 为每个事件赋予几个不同的优先级：

LOG_EMERG--紧急情况

LOG_ALERT--应该被立即改正的问题，如系统数据库破坏

LOG_CRIT--重要情况，如 IO 错误

LOG_ERR--错误

LOG_WARNING--警告信息

LOG_NOTICE--不是错误情况，但是可能需要处理

LOG_INFO--情报信息

LOG_DEBUG--包含情报的信息，通常旨在调试一个程序时使用

例如：

#Sep 11，23：09：53 这时网卡地址为 00:00:e2:6f:26:9b 的设备通过内网得到 DHCP 服务分配的地址 192.168.138.150

Sep 11 23:36:57 gw1 authpriv.info in.telnetd[663]: connect from 192.168.138.248

Sep 11 23:37:00 gw1 auth.info login[664]: root login on `ttyp1' from `192.168.138.248'

#Sep 11，23：37：00 用户 root 从 192.168.138.248 登录。

日志中的**”--MARK--”消息**：在默认情况下每隔 20 分钟就会生成一次表示系统还在正常运行的消息。**”-- MARK --”**消息很像经常用来确认远程主机是否还在运行的“心跳信号”(Heartbeat)。



第五章 Console 配置

APN OLYM2008 系列产品支持 Console 配置方式，本章介绍如何使用 windows 系统超级终端控制台程序配置设备。

连接

Console 配置方式硬件接线图示：

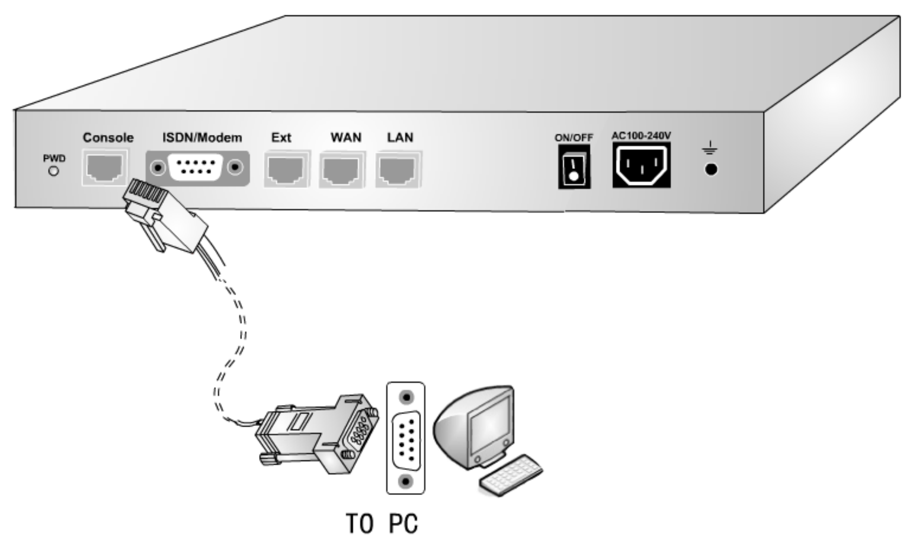


图 5-1：Console 连线图

配置电脑

以 Windows XP 为例。在“开始”→“程序”→“附件”→“通讯”→“超级终端”，启动超级终端程序。

1. 新建连接，新建 OLYM，如下图示：



图 5-2：新建超级终端连接

2. **选择正确的 COM 口**。根据实际连接接口，选择正确的 COM 口（连接计算机使用的串口），如下图示：



图 5-3：连接的 COM 口选择

3. **COM 口属性配置**。如下图示：



图 5-4：COM 属性配置

选择端口后，选择确定，需要设置通讯的

- 波特率为 9600
- 数据位　8
- 奇偶校验 无
- 停止位　1
- 数据流控制 无

注意： 如果 Console 线与电脑 COM2 口连接，则在超级终端连接接口选择时应选择 COM2 口。

基本设置

系统正常引导启动后。初次登陆配置，在提示登陆处输入缺省帐号：

APN STAR66 5.0

GW2 login: ***root***

Password: ***gw1admin***（屏幕不显示）

成功登陆后，显示如下：

Welcome to OLYM-APN,　APN Configuration:

APN STAR66 Release 5.0

fw3.0, kernel 2.4.18 arca2

win v3.0

WEB V2.0

Build No: 808401.20071009

----

help : for a help menu

version : for show APN GW Configuration

[STAR66:test020 /]# ***setup***

进入配置界面：

```
GW CONFIG

AUTHCYBER.COM   GW1 CONFIG
   Copyright (C) 2001-2016, All right reserved
You should read the INSTALL MANUAL first,   Enter: setup for this
If you are first time to config it on the step 1,2,3,4
The   GW configuration choices are:
1 -   GW LICENSE   (VDOMAIN/VHOST/LICENCE/VPUBKEY)
2 -   LAN NETWORK (LAN IP/MASK)
3 - WAN LINK (ADSL/DDN/ISDN/Dial-up)
4 - SAVE RUN_CONFIG TO START_UP_CONFIG
0 - EXIT CONFIGURATION:   Exit to system prompt.
Your choice?
```

图 5-5：命令行配置菜单

初次使用或者系统处于缺省配置状态下，请按照 1，2，3，4 的次序来进行系统配置。

1-GW LICENSE(VDOMAIN/VHOST/LICENCE/VPUBKEY)： 许可证（组域名/节点名/许可证/预共享密钥）

Your choice ***1***

Every GW have a unique VDOMAIN/VHOST License

GW at the same VDOMAIN and Authenticate PSK

can communication to each other.

GW VDOMAIN(Default:unkonw): ***your domain***

GW VHOST(Default: unknow): ***your host***

GW LICENCE (Default: LICECESNUST24BYTES):***your license***

Authenticate PSK(Default: public):***pre-share Key***

** Summary of what you entered **

AUTHBY = Pre-share-key

GW VDOMAIN : demo

GW VHOST : demohost

LICENCES : WrWtg4gk6O8rPowd7qqn4j

Authenticate PSK : public

Accept these settings and adjust configuration files (y/n)? ***y***

2-LAN NETWORK(LAN IP/MASK)：局域网（LAN IP/子网掩码）

Your choice ***2***

GW IP Address
Enter the IP address of the Internal network
(default 192.168.0.63): ***192.168.250.10***

GW IP Address Netmask
Enter the IP Netmask of connected to the internal network
(default 255.255.255.0): ***255.255.255.0***

** Summary of what you entered **
GW IP Address: 192.168.250.10
Netmask: 255.255.255.0

Accept these settings and adjust configuration files (y/n)? ***y***

3- WAN LINK (ADSL/DDN/ISDN/Dial-up)：广域联接（ADSL/DDN/ISDN/Dial-up）

```
  WAN: Select the way to link to Internet
1 - Dialup        : Use Extend Modem Link to Internet
2 - ISDN          : Use ISDN TA Link to Internet Must a extend device
3 - ADSL          : ADSL Link to Internet
4 - DDN/FIX IP    : DDN or other lease line link to Internet have fix ip
0 - EXIT TO Main: Return to main menu

Your choice?
```

图 4-4：网络连接方式

选取 1 -Dialup， 进行拨号上网方式的有关配置：

Enter the phone number of your ISP
Phone Number: ***163***
Enter your dial-up username
Username: ***163uid***
Enter your dial-up Password
Password : ***163passwd***
** Summary of what you entered **
Dial Up Number : 163
Dial Username : 163uid
Dial Password : 163passwd
Accept these settings and adjust configuration files (y/n)? ***y***

注意：

- ❶ 以上信息可能会因设备版本的不同而略有些差异，但配置方式适合所有版本。
- ❶ 当采用电话拨号方式时，对于是通过分机上网的，要在被拨的电话号码前加拨外线的号码及一个”，”号。如拨外线的号为”9”，拨 163 的电话可以拨：”9,163”。

选取 2 -ISDN ，与 ISDN TA 进行互联的方式。

同 1。

选取 3 -ADSL，与 ADSL Cable Modem 进行联接的方式。

Enter your PPPoE user name

Username: (default uid@163.gd): ***your_username@163.gd***

Enter your ADSL Password

Password : ***password***

** Summary of what you entered **

PPPoE User name : your_username@163.gd

Password : passwdhere

Accept these settings and adjust configuration files (y/n)?***y***

选取 4 -DDN/FIX IP，具体配置如下：

DDN IP Address

Enter the IP address of the Internal network

(default 172.168.250.250): ***202.104.177.177***

GW IP Address Netmask

Enter the IP Netmask of connected to the internal network

(default 255.255.255.0): ***255.255.255.240***

** Summary of what you entered **

DDN IP Address: ***202.104.177.177***

Netmask: ***255.255.255.240***

Accept these settings and adjust configuration files (y/n)? ***y***

4 - SAVE RUN_CONFIG TO START_UP_CONFIG：保存配置

注意： 做完配置敬请进行保存，否则系统启动后会自动恢复到上一次存取的状态。

设置步骤小结

如果是首次使用 Console 方式配置设备，参考下面的小结 5 分钟可以完成配置。这里以设置 ADSL 拨号上网为例。

第一步　用 root 作为用户名，gw1admin 作为初始密码进入系统，键入 setup；
第二步　选择 1，输入 vdomain，vhost 和 licenses；
第三步　选择 2，设置连接内部网络的 eth0 接口卡的 IP 地址和子网掩码；
第四步　选择 3，再选择 ADSL，输入用户名和密码；
第五步　选择 4，保存以上设置；
第六步　重启设备（关闭电源，　两秒后再开启电源）。

第六章　VDN 服务及管理

本章主要介绍设备终端之间建立自动隧道的简单过程。

VDN 服务介绍

VDN 服务是由服务商 VDN 服务器或者带有 VDN 模块的 APN OLYM2008 设备提供，使用 VDN 服务可以实现全动态 VPN 网络，并且可以方便的集中管理和网络调整，用户配置时只需要短短的几分钟即可使用 VPN 隧道通讯。

(一) 设备终端自动隧道建立过程

例如：　某客户在两地有两个局域网，分别为 A 网络和 B 网络（以下简称 A、B），现在需要 A 跟 B 能通过 Internet 进行安全连接，并能相互通信。

根据需求分析，需要在 A、B 两边安装 APN OLYM2008 终端设备，分别通过 ADSL 或专线等上网线路接入互联网。

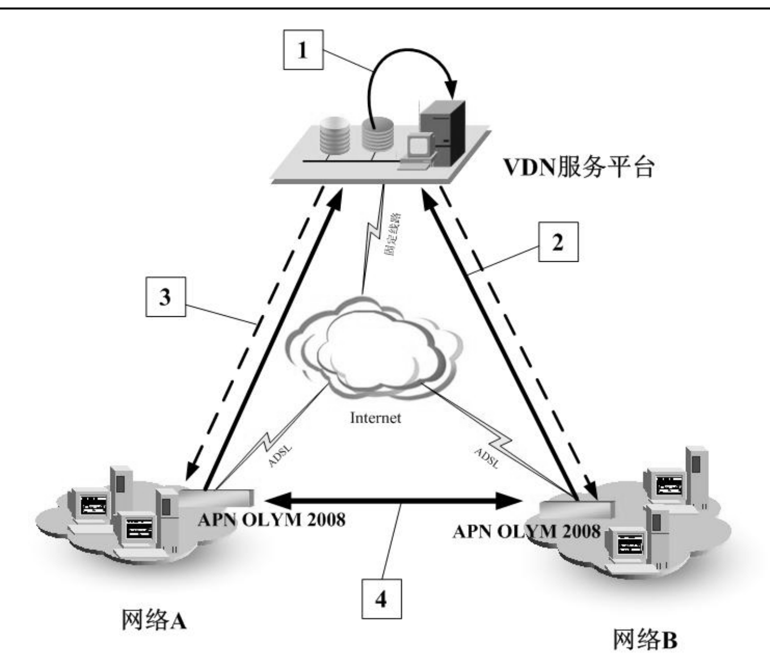


图 6-1：工作原理图

(二) VDN 服务平台上发放许可证

如上图 1 标志所示。在 VDN 服务平台上为此客户生成唯一能够标识其网络的组域名（Vdomain），例如：olymcor，然后在 olymcor 域下，为 A、B 终端设备分别生成节点（Vhost），例如：siteA、siteB。同时，服务系统会自动产生一个 24 位长的 license 随机数据，例如：IGo9TTZQ7ITJvlFbKCK0JMUw。

如上述过程，在 VDN 管理平台上产生了一个使用设备的客户信息：

1. 用户信息：xxxx 有限公司；
2. 组域号：olymcor；
3. 节点名称：siteA、siteB
4. license 信息：

组域名　：olymcor

编号	组域名	节点名	许可证号
1	olymcor	siteA	yVXaXxShHsegZt4ZF6SqupK5
2	olymcor	siteB	Ddwn9Yg6swuhZy9jjw0Zw9nQ

5. 设备终端到 VDN 管理中心的认证

如上图标志 2 所示。在对设备终端进行初始配置时，需要设置相对应的组域号、节点名及 license。当终端设备成功连接至互联网后，自动根据以上的信息到所属的 VDN 服务平台进行身份认证。

设备通过 VDN 服务中心认证后，会将公网 IP、内网网段等信息登记到 VDN。VDN 根据设备所在组域产生一张所有节点认证后的在线信息表。

(三) VDN 管理中心下发信息给 设备终端

如上图标志 3 所示。VDN 管理中心根据设备登记的信息生成域的在线信息表后，自动生成两端设备建立通信隧道所需要的 IKE 协商参数，并下发到设备终端设备上。

将 IKE 协商所需要的配置由 VDN 管理平台下发给终端，可以做到：

1. 用户不需要在终端设备上进行复杂的配置，使复杂的 IPSec IKE 配置过程对用户透明化；
2. 当在网络中新增节点 siteC 时，只需在 VDN 服务平台上该域下为 siteC 分发 license 即可，新节点设备认证后，可迅速由 VDN 服务平台下发原有节点的信息，达到了快速部署大规模网络，扩展容易的特点；
3. 终端设备每次成功连接互联网后，都重新主动的到 VDN 服务平台认证，然后获得 VDN 管理中心下发的其他在线节点的信息，解决了全动态 IP 建立隧道的问题；
4. VDN 平台上，可以设置组域内各节点之间逻辑连接关系，比如在 VDN 上建立以 siteA 为中心点的星型拓扑关系。VDN 服务平台根据组域所对应的关系定义规则来决定下发的信息。

注意：

如果组域内没有进行关系定义，域内所有节点之间建立一种全网状关系。一旦定义了一条关系定义规则，VDN 管理中心将严格按照关系定义的规则下发信息。

(四) 设备终端之间进行 IKE 协商建立安全通信隧道

如上图标志 4 所示。 设备终端获得跟对方终端进行 IKE 协商所需要的参数后，由 VDN 管理中心协调其中一方发起 IKE 协商过程，建立两端安全通信隧道。

注意：

❶ 当两端 设备设备外网口都为公网 IP 地址，IKE 协商使用 UDP 500 端口；而当一端设备外网口为公网 IP，另一端为私网 IP（如小区宽带共享的 NAT 上网方式），IKE 协商使用 UDP 500 端口和 UDP 4500 端口；

❷ 隧道建立起来后，两端 设备设备外网口都为公网 IP 地址，数据包通过 ESP 协议封装后传送到互联网；而当一端设备外网口为公网 IP，另一端为私网 IP（如小区宽带共享的 NAT 上网方式），数据包还需要通过 UDP 4500 封装后传送到互联网；

❸ 设备终端之间建立安全通信隧道后，两端网络进行通信的数据，不会经过 VDN 管理中心；

VDN 管理简介

（一） Cache 值计算

Cache 值是 VDN 地址通过其自身的解析功能解析到的一个数字串，在 APN OLYM2008 管理界面又称为主识别号，它和 VDN 地址是一一对应关系。

如果企业自己有 VDN 服务器，那么首先必须把当前 VDN 的固定 IP 地址解析为 cache，具体做法如下：

通过 Telnet 或 Console 方式进入设备命令行，使用如下命令：

#conv ***xx.xx.xx.xx***（VDN 外网口固定 IP）

（二） 许可证生成管理

生成许可证前必须先为客户建立用户信息，例如，为用户"test"建立用户信息，就可以"为此用户新建组域"如下图示：

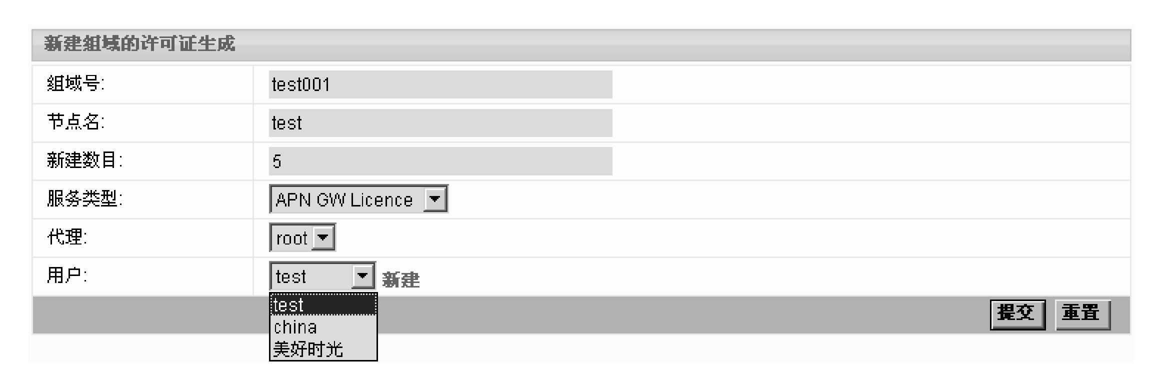


图 6-2：许可证生成

（三） 拓扑关系定义管理

拓扑关系定义是 VDN 平台进行

組域号: test001 结点关系定义 在线结点详细信息 输出纯文本格式

组域列表

組域号	节点名	在线数	许可证号	类型	端口	机号	最后更改日期	代理商	用户	控制	编辑
test001	123	.	VwPtUOXG6dFJIfQWIR0JAAbC	2	8401	0	20071214151351	root	test	0	edit
test001	host001001	28	IwwMH1B381Nnjv6ou7VDTkFF	2	8401	0	20071207170838	root	test	0	edit
test001	host001002	.	xu1bwEIP1gRdIHu0VQ4IVpA6	2	8401	0	20071207170838	root	test	0	edit
test001	host001003	.	0xqL7Hmw5XdX27DkSgJYOObE	2	8401	0	20071207170838	root	test	0	edit
test001	host001004	.	YTMUs0mQbkodEWnPb2IdcRPx	2	8401	0	20071207170838	root	test	0	edit
test001	host001005	.	Of2oxxeMaeoRVkvNOESIVtrw	2	8401	0	20071207170838	root	test	0	edit
合计:	6	1								添 加	

图 6-3：组域信息列表

如图示，点击"节点关系定义"进入下图为组域 test001 建立以 test001001 节点为中心点名的逻辑拓扑结构，设置如下示：

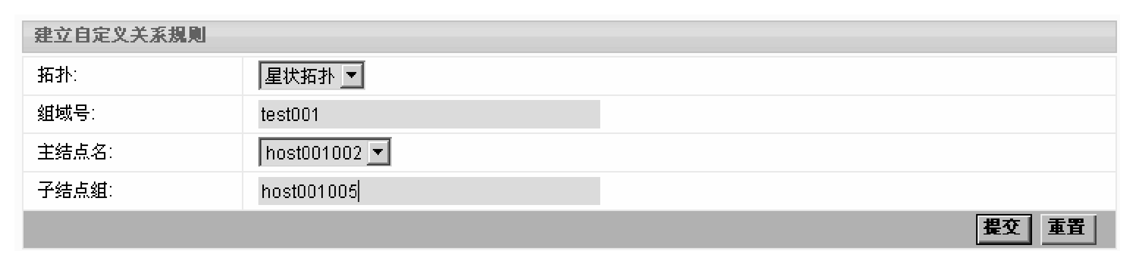


图 6-3：节点关系定义

添加完成点击"提交"如下图示，当前组域 test001 的虚拟网络为以 test001001 为中心点的星状结构。

組域号: test001 报警事件

組域号	拓扑	主节点名	子节点組	建立时间	删
test001	星状拓扑	host001001	{全部}	2007.12.10 09:07	x
test001	星状拓扑	host001002	host001005	2007.12.14 15:53	x
合计:	2			添 加	

图 6-4：拓扑关系列表

（四） 报警事件管理

VDN 平台上可以针动特定 VDOMAIN 或 APNGW 机器的事件报警定义．当定义的事件被触发时，系统会产生待做事件列表，从而作为主动服务的待处理事务池，用于提供主动的 APN 服务，报警管理包括：事件定义、事件处理及事件报警。

进入“事件定义”进入当前报警事件列表，为组域 “添加”新报警事件，如下图示

組域号:test001 报警事件

組域号	子节点組	报警条件	建立时间	删
test001	{全部}	巡检警告	2007.12.10 09:18	x
test001	{全部}	重联或APN离线	2007.12.10 09:25	x
test001	host001001	在 0:0 时未接入	2007.12.10 09:25	x
合计:	3			添 加

图 6-5：报警事件列表

（五） 保存配置

每做完一次 VDN 服务操作管理，都必须进入“许可证”→“配置保存”操作，否则当服务器重启后，上次所作所有信息操作将会丢失。

第七章　局域网工作站设置

本章将简单指导如何进行计算机网络设置

Windows XP 工作站设置举例

点击 “开始“→“设置”→“网络连接”→“本地连接”，出现如下图所示

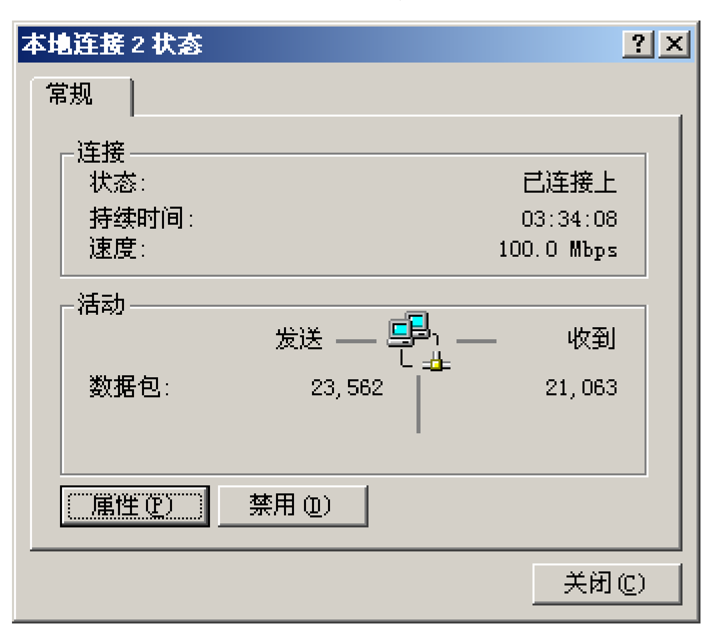


图 7-1：本地连接状态

进入“属性”对话框，选择“Internet 协议 TCP/IP”双击或者点击“属性”按钮进入如下图，



图 7-2：本地连接属性

选择"使用下面的 IP 地址（S）"分别设置：IP 地址、子网掩码、默认网关（ 设备内网口 IP 地址）。

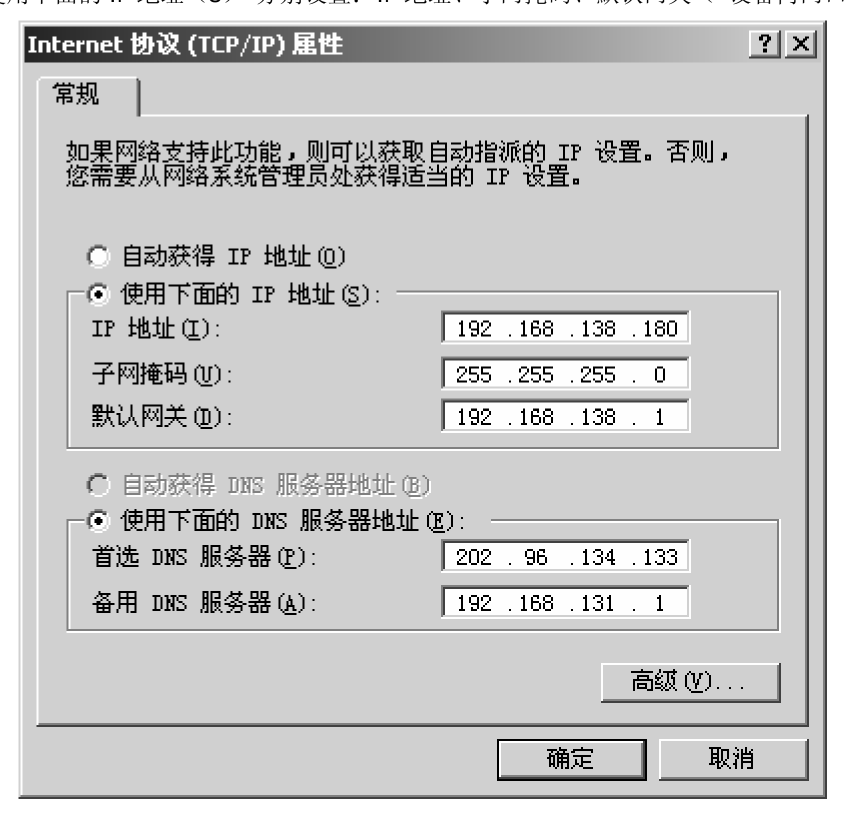


图 7-3：Internet 协议（TCP/IP）属性

DNS 服务器设置“首选 DNS 服务器”一般为本地 ISP 的 DNS 地址，有必要设置备用 DNS 服务器地址，设置完成可能需要按照计算机系统提示重启才会生效。

提示：如果设备启用了 DHCP/DNS 服务，可采用“自动获得 IP 地址”选项，这样就不需要做任何设置。

第八章　常见问题解答

本章列举了部分常见的问题。更多FAQ，敬请参考www.olymtech.net 。

忘记密码怎么办?

APN OLYM2008 系列产品均支持密码恢复按键 PWD。当不小心忘记密码时，请在加电情况下按住机箱背板上的 PWD 按键 10 秒钟左右，此时系统密码及内网口 IP 均可恢复至出厂配置。

即此时设备地址恢复为 192.168.32.200 ，登陆用户名 root，密码 gw1admin。

注意：按键完成后不能重启设备。否则又恢复成为原来设置的密码。此时设置新密码后保存重启即可使用新的密码登录。

设备面板指示灯不同闪亮情况代表什么意思?

APN OLYM2008 设备 Status 由 4 盏 LED 灯组成，当前支持中间两盏灯状态组合的异常报告，下面是 Status 灯状态含义：

Status 灯状态	表达意思
由左到右闪烁，时间间隔为 2 秒	设备运行正常
左灯灭，右灯闪烁	外网连接异常，如：ADSL 不正常
由左到右闪烁，中间没有间隔，频率快	许可证不能成功接入
由右到左闪烁，中间没有间隔，频率快	内网口地址段跟其他节点冲突
使用过程中两灯状态都不变化	设备锁死

当故障发生时，可先通过 SYS 灯显示出的状态和网络接口指示灯来初步判断故障。

设备一开机 Status 灯状态不对，这是怎么回事?

这是正常的，不同硬件可能出现 Status 灯会全亮或全不亮的情况，设备初始化完成后就会进入正常闪亮状态。

如何查看当前设备接口连接状态及其 IP 地址?

在 Web 管理界面，进入“系统管理”→ “系统信息”查看“公网 IP”或者“局域网 IP”。

如何确认自动隧道已成功建立？

使用自动隧道时，点击 APN 的 Web 管理界面的"虚拟专网"，许可证处显示，如：

当前 APN 组域：zjtz

节点名: host001

状态: 已成功接入【此状态显示已经成功获得认证，可以使用自动隧道】

主识别号: 2362139603

注意状态提示：如未成功接入，请点击"许可证号"手动激活或重启设备，当多次仍不能成功接入请拨打服务支持电话。

当许可证显示"已成功接入"而无隧道信息时，该如何处理？

请尝试按照以下方法步骤处理：

1. 检查对端节点是否成功接入；
2. 如"已成功接入"请确认双方预共享密钥相同；
3. 如果是动态获得地址，重启设备，更换外网 IP。

当有隧道信息但隧道状态显示"Hold"时，该如何处理？

请尝试按照以下方法步骤：

1. 请进入"网络接口"→"重联广域网"；
2. 重启设备更换外网 IP。

局域网不能上网时如何处理？

请先查看设备面板的 WAN 和 Status 指示灯状态：

当 Status 为左灯灭，右灯闪烁时，此时是外网故障，尝试：

1. 检查 APN 外网联线是否正常；
2. 重启 APN OLYM2008 设备和 Modem；
3. 重启后如果不能恢复正常，请使用单台电脑检查上网线路是否正常。如果不正常，请联系运营商解决；

当 Status 两灯状态交替 2 秒闪烁，此时设备运行正常，尝试：

1. 检查不能上网的计算机的配置（IP 地址，网关，DNS 设置），并且测试是否能 ping 通网关（APN 内网口 IP）；
2. 重启设备，如果能恢复正常，请注意检查"系统资源"和"当前会话"信息报告，确定内网是否存在电脑感染病毒（如 ARP 病毒）不断往外发包的情况，大量往外发包会致使 ISP 封 IP 情况出现；

如果还不能解决问题，请拨打服务支持电话。

能上网但不能和其他节点的主机或服务器通信，该如何处理

a 点击 Web 管理界面的"虚拟专网"检查是否有其他节是否上线；

b 如果未显示"成功接入"或者无任何隧道信息，请点击"虚拟专网"→"许可证号"，选择"现在激活"后，按"提交"按钮；

c 等待 2 分钟左右，重新检查注册情况和隧道情况，如果还不能正常，请打服务支持电话。

ADSL 无法拨号上网

1. 检查网线是否使用正确。大多数 ADSL Modem 使用普通网线直接与设备的 WAN 口相连。
2. 检测用户名和帐户是否正确或被盗用。请按照 ISP 提供的用户名和帐户输入。
3. 部分地区的 ADSL 用户，在终端设备突然掉电之后，不能马上拨号。需要等待一会才能重新连接。
4. 确认 Modem 是处于路由模式还是透明模式。Modem 如是路由模式请修改为透明模式，由 APN 来进行 PPPOE 拨号。
5. 查看智能向导中的提示信息。

ADSL 线路不是很稳定，常常断线怎么办?

当前 adsl 一般使用 pppoe 拨号，拨号成功后拨号程序会不断的发送 LCP（链路控制协议）包来维护这个 ppp 连接。如果 ADSL 线路过长，或者线路质量不好、adsl modem 故障等，都容易导致 LCP 数据包发送和接收异常，造成连接中断。

1. 检查内网是否有病毒造成大量往外发包，或者内网有使用 BT 等 p2p 工具下载造成上下行数据量较大、或者内部计算机较多正常访问量很大、ADSL 不能满足带宽要求等。这些情况都易导致 ADSL 导致 ADSL 容易出现断线重拨；
2. ADSL 线路本身不稳定，容易断线重拨，可使用电脑拨号进行验证，或查看设备日志；线路问题请及时联系线路服务商获得支持。

连接 Internet 前可以进入 Web 界面，但后来局域网工作站不能上网，也不能进入 web 界面

如果设备 Status 指示灯状态为：由右到左闪烁，中间没有间隔，频率快，则说明网络地址发生冲突。请重新规划本地 IP 或者协调整个网络的 IP 规划。

注意：同一个 Vdomian 内不同 Vhost 设备的 LAN IP 不能处于同一个网段。

设备正常运行过程中突然网口指示灯没有任何指示了，该如何处理?

请按照下面步骤进行问题排除：

a 重启 APN OLYM2008、ADSL Modem 和内网交换机等设备；

b 如果问题不能解决，请更换相应的网线，并且确认已经接触良好，相应的指示灯都正常；

c 如果还不能解决问题，请打服务支持电话。

使用设备不能正常拨号上网，但是某台计算机可以拨号是怎么回事?

此种情况很可能是 ISP 将上网方式绑定计算机 MAC 地址的原因。APN OLYM2008 设备支持外网接口卡（网卡）的 MAC 地址修改，请参考第四章 MAC 地址修改内容部分。

可以放在防火墙之后吗?

APN OLYM2008 系列设备本身具备强大的防火墙功能，已通过防火墙安全检测并获得了防火墙销售许可证书。可与任何网络设备结合使用。当希望与防火墙配合使用时，可以放置其前或其后，也可以与其并联使用。